



Minister van Justitie en Veiligheid en
Staatssecretaris Rechtsbescherming
Postbus 20301
2500 EH DEN HAAG

Datum
3 maart 2025

Ons kenmerk
z2024-014439

Uw brief van
8 mei 2024

Contactpersoon

Uw kenmerk
5439659

Onderwerp

Modernisering Wetboek van Strafvordering - Wetgevingstoets conceptwetsvoorstel Eerste aanvullingswet nieuw Wetboek van Strafvordering

Geachte heer Van Weel, geachte heer Struycken,

Bij brief van 8 mei 2024 is de Autoriteit Persoonsgegevens (hierna; AP) conform artikel 28, tweede lid, van de Richtlijn gegevensbescherming bij rechtshandhaving¹ (hierna: RGR) geraadpleegd over het conceptwetsvoorstel voor de Eerste aanvullingswet nieuw Wetboek van Strafvordering (hierna: het concept). Dit concept bevat wijzigingen en aanvullingen van de op 20 maart 2023 respectievelijk op 16 oktober 2024 ingediende voorstellen voor twee vaststellingswetten voor het nieuwe Wetboek van Strafvordering en vormt aldus onderdeel van een omvangrijk wetgevingsproject tot modernisering van het Wetboek van Strafvordering.

Omdat de AP laatstelijk in juli 2018 over de modernisering van het Wetboek van Strafvordering heeft geadviseerd en nadien belangrijke ontwikkelingen met betrekking tot het Europese gegevensbeschermingsrecht in het domein van de rechtshandhaving hebben plaatsgevonden, maakt de AP van deze gelegenheid gebruik om niet alleen te reageren op de voorgelegde bepalingen, maar ook opmerkingen te maken over een aantal belangrijke onderwerpen betreffende de bescherming van persoonsgegevens die in de voorstellen voor het nieuwe wetboek nog onvoldoende hun weerslag hebben gevonden. Als gevolg hiervan en door de omvang en complexiteit van dit wetgevingsproject alsmede de

¹ Richtlijn 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

eerdergenoemde Europese rechtsontwikkelingen in dit domein in deze periode, heeft het uitbrengen van deze wetgevingstoets meer tijd in beslag genomen dan gebruikelijk.

Inhoud wetgevingstoets

Deze wetgevingstoets bestaat uit de volgende onderdelen:

1. Conclusie
2. Hoofdlijn
3. Verloop wetgevingsproject modernisering Wetboek van Strafvordering
4. Strekking van het voorliggende concept
5. Wetgevingstoets
 - 5.1 Algemeen
 - 5.2 Het Handvest van de grondrechten van de EU en de Richtlijn gegevensbescherming bij rechtshandhaving
 - 5.2.1 Het Handvest van de grondrechten van de Europese Unie
 - 5.2.2 De Richtlijn gegevensbescherming bij rechtshandhaving
 - 5.3 Relevante rechtspraak van het Hof van Justitie
 - 5.3.1 Bevel tot verstrekking van (persoons)gegevens
 - 5.3.2 Onderzoek aan digitale-gegevensdragers en geautomatiseerde werken
 - 5.3.3 Stelselmatig verzamelen, opslaan en gebruiken van biometrische gegevens
 - 5.4 Verwerking van verzamelde persoonsgegevens
 - 5.4.1 Bewaren en vernietigen van persoonsgegevens
 - 5.4.2 Doelafwijkend gebruik van persoonsgegevens
 - 5.4.3 Verwerking van bijzondere persoonsgegevens
 - 5.4.4 Verwerking van ANPR-kentekengegevens
 - 5.4.5 Onderzoek en geautomatiseerde data-analyse van persoonsgegevens
 - 5.4.6 Doeltreffende voorziening in rechte en notificatieplicht
 - 5.4.7 Verhouding Wetboek van Strafvordering tot Wpg en Wjsg
 - 5.5 Overige opmerkingen ten aanzien van het concept
6. Werklast AP
7. Openbaarmaking

1. Conclusie

De AP heeft bezwaar tegen het voorliggende concept. De AP constateert dat met de voorstellen voor het nieuwe Wetboek van Strafvordering de mogelijkheden om grote hoeveelheden (digitale) persoonsgegevens voor de opsporing te verzamelen en te gebruiken substantieel worden uitgebreid terwijl de waarborgen met het oog op het recht op bescherming van persoonsgegevens en het recht op eerbiediging van de persoonlijke levenssfeer die daarmee gepaard zouden moeten gaan, onvoldoende zijn en achterblijven bij de Europese rechtsontwikkeling. Hierdoor ontbreekt een goede balans tussen enerzijds het belang om strafbare feiten op te sporen en ernstige criminaliteit effectief te bestrijden en anderzijds de noodzaak om de in het Unierecht verankerde fundamentele rechten en vrijheden van



Datum
3 maart 2025

Ons kenmerk
z2024-014439

betrokkenen, waaronder met name ook betrokkenen die met strafbare feiten niets van doen hebben, te waarborgen en te beschermen. De AP acht daarom wijziging en aanvulling van het nieuwe Wetboek van Strafvordering noodzakelijk teneinde strijdigheid met het Unierecht te voorkomen. Gebeurt dit niet, dan bestaat het reële risico dat bepalingen uit het nieuwe wetboek wegens strijdigheid met het hogere recht in concrete gevallen buiten toepassing moeten blijven.

2. Hoofdlijn

- **Balans tussen efficiënte opsporing en bescherming van fundamentele rechten dreigt verloren te gaan.** Het concept houdt onvoldoende rekening met de gevolgen van de (grootschalige) gegevensverwerkingen die voortvloeien uit de bevoegdheden die in het nieuwe wetboek worden opgenomen en de waarborgen die in dat verband nodig zijn om de fundamentele rechten en vrijheden van personen, waaronder personen die geen enkele betrokkenheid bij strafbare feiten hebben, te waarborgen.
- **Voorkomen moet worden dat (gevoelige) gegevens over niet-verdachte personen zonder legitieme redenen in de politiesystemen belanden.** Dit zou niet alleen een ernstige inbreuk in het grondrecht op bescherming van persoonsgegevens opleveren, maar kan ook grote risico's voor deze personen met zich meebrengen. Bijvoorbeeld wanneer die gegevens voor hele andere doelen worden gebruikt, met andere partijen worden gedeeld, in verkeerde handen vallen of uit die gegevens onjuiste conclusies worden getrokken.
- **Wetgeving moet aansluiten bij de op Europees niveau ontwikkelde waarborgen.** Het nieuwe Wetboek van Strafvordering blijft achter bij de Europese rechtsontwikkeling. Dit is problematisch omdat daardoor Europese waarborgen met betrekking tot het recht op bescherming van persoonsgegevens en het recht op eerbiediging van de persoonlijke levenssfeer niet in het nieuwe wetboek worden geïncorporeerd. Daardoor dreigt het nieuwe Wetboek van Strafvordering niet aan het vereiste niveau van rechtsbescherming te voldoen en een voor de praktijk onwenselijke situatie van rechtsonzekerheid te ontstaan.
- **In meer gevallen moet worden voorzien in voorafgaande toetsing door de rechter-commissaris.** De Europese regelgeving zoals uitgelegd door het Hof van Justitie, dwingt tot aanpassing van de bepalingen in het voorstel voor vaststellingswet I en nadere doordenking van de gekozen systematiek. Om de rechten en vrijheden van betrokkenen op het juiste niveau te waarborgen, moet in ieder geval een voorafgaande toetsing door een rechter-commissaris (of een onafhankelijke bestuurlijke autoriteit) worden ingevoerd voor:
 - het bevel tot verstrekking van persoonsgegevens bij een aanbieder van communicatiediensten (zie paragraaf 5.3.1);
 - het bevel tot verstrekking van PNR/passagiersgegevens bij de passagiersinformatie-eenheid (zie paragraaf 5.3.1);
 - het onderzoek aan een digitale-gegevensdrager of geautomatiseerd werk (zie paragraaf 5.3.2);
 - het bevel tot raadpleging en verstrekking van ANPR-kentekengegevens (zie paragraaf 5.4.4).
- **Regeling van het stelselmatig afnemen en opslaan van gezichtsopnamen en vingerafdrukken kan niet in stand blijven.** Ook op dit punt dwingt de Europese regelgeving en de uitleg die het Hof van Justitie daaraan geeft tot aanpassing van wetgeving. De huidige regeling van het stelselmatig afnemen en



Datum
3 maart 2025

Ons kenmerk
z2024-014439

opslaan van gezichtsopnamen en vingerafdrukken ten behoeve van de opsporing van (toekomstige) strafbare feiten en het (geautomatiseerde) gebruik van deze biometrische gegevens kan niet in stand blijven. Verwerking van deze bijzondere persoonsgegevens is namelijk alleen toegestaan als dit strikt noodzakelijk is en hiervoor een duidelijke en nauwkeurige grondslag bestaat (zie paragraaf 5.3.3).

- **Persoonsgegevens die niet-relevant zijn voor het onderzoek moeten meteen worden vernietigd.** De regeling voor het bewaren en vernietigen van met opsporingsbevoegdheden vergaarde persoonsgegevens (artikel 2.1.18 en 2.1.19) dient te worden aangescherpt en uitgebreid, zodat persoonsgegevens van personen die geen enkele betrokkenheid hebben bij strafbare feiten worden vernietigd en voorkomen wordt dat deze in de politiestructuren bewaard blijven. (Zie paragraaf 5.4.1.)
- **Er moeten meer waarborgen komen voor het doelafwijkend gebruik van met opsporingsbevoegdheden verzamelde persoonsgegevens.** De regeling moet in de eerste plaats in lijn worden gebracht met de RGR en het evenredigheidsbeginsel waarbij de doelen waarvoor dergelijke gegevens verder kunnen worden gebruikt in redelijke verhouding moeten staan met de inbreuk die met de verdere verwerking wordt gemaakt op de grondrechten van de bij die verdere verwerking betrokken personen. De AP ziet hierbij een toetsende rol voor de rechter-commissaris weggelegd. Ook is een duidelijker en nauwkeuriger formulering van de bepalingen vereist. (Zie paragraaf 5.4.2.)
- **Regels voor het inrichten, vullen en gebruiken van databanken met o.a. gezichtsopnamen, vingerafdrukken en DNA-profielen die worden gebruikt voor de opsporing van (toekomstige) strafbare feiten moeten op het niveau van de wet worden vastgesteld.** Verwerking van bijzondere persoonsgegevens, in het bijzonder in de vorm van opname in een databank voor de opsporing van toekomstige strafbare feiten en raadpleging van die databank, dient op het niveau van een wet in formele zin te worden geregeld, waarbij die verwerking dient te voldoen aan het vereiste van strikte noodzakelijkheid en evenredigheid. Een afzonderlijke kaderwet hiervoor verdient overweging. (Zie paragraaf 5.4.3.)
- **Er moeten regels komen voor geautomatiseerde data-analyse en onderzoek aan grote (bulk)gegevensbestanden.** In het wetboek moet een regeling worden opgenomen die onderzoek en geautomatiseerde data-analyse van (bulk)gegevens normeert. Naar het oordeel van de AP zou in deze regeling nadrukkelijk een toetsende rol van de rechter-commissaris moeten worden opgenomen. Deze regeling dient gelijktijdig met de inwerkingtreding van de bevoegdheden tot het vergaren van persoonsgegevens in werking te treden. (Zie paragraaf 5.4.5.)
- **Een doeltreffende voorziening in rechte moet zijn verzekerd.** Informatie aan de betrokkene is hierbij een voorwaarde. Er moet een nadere analyse komen van de bepalingen in het wetboek en in de Wpg en de wijze waarop daaraan in de praktijk uitvoering wordt gegeven. Zo nodig moeten de wet en/of de uitvoeringspraktijk worden aangescherpt om dit grondrecht te verzekeren. (Zie paragraaf 5.4.6.)
- **De verhouding tussen het Wetboek van Strafvordering en de Wpg/Wjsg moet duidelijk zijn.** Uit de tekst van de wet en de toelichting moet duidelijk worden hoe de bepalingen over bewaren, vernietigen en doelafwijkend gebruik in het nieuwe Wetboek van Strafvordering zich verhouden tot vergelijkbare bepalingen in de Wpg en de Wjsg. (Zie paragraaf 5.4.7.)



Datum
3 maart 2025

Ons kenmerk
z2024-014439

3. Verloop wetgevingsproject modernisering Wetboek van Strafvordering

Dit advies betreft het derde advies van de AP in het kader van de modernisering van het Wetboek van Strafvordering. Eerder bracht de AP adviezen uit op 23 oktober 2017 over Boek 1 en 2 en laatstelijk op 10 juli 2018 over Boek 3 t/m 6. De desbetreffende conceptwetsvoorstellen zijn samengevoegd en als voorstel voor een eerste vaststellingswet (hierna: vaststellingswet I) op 20 maart 2023 bij de Tweede Kamer ingediend.²

Het voorstel voor de tweede vaststellingswet (hierna: vaststellingswet II) dat op 16 oktober 2024 bij de Tweede Kamer is ingediend betreft Boek 7 en 8.³ Dit wetsvoorstel is ten onrechte niet voor toetsing aan de AP voorgelegd. Uit artikel 28, tweede lid, van de RGR vloeit de *verplichting* voort de AP te raadplegen bij het opstellen van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel of een daarop gebaseerde regelgevingsmaatregel in verband met de verwerking van persoonsgegevens die onder de reikwijdte van die richtlijn valt. Ook het voorstel voor vaststellingswet II bevat bepalingen betreffende de verwerking van persoonsgegevens, zoals bijvoorbeeld over de doorgifte van persoonsgegevens aan derde landen.⁴ De AP overweegt alsnog ambtshalve een wetgevingstoets over dit wetsvoorstel uit te brengen.

Aanvankelijk bestond het voornemen om ook een nieuwe gegevensverwerkingswet op het terrein van politie en justitie tot stand te brengen ter vervanging van de Wet politiegegevens (hierna: Wpg) en de Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg). De Commissie Koops - die in opdracht van het ministerie van Justitie en Veiligheid voor de modernisering van het Wetboek van Strafvordering onderzoek deed naar de regulering van opsporingsbevoegdheden in een digitale omgeving - kwam in 2018 al met de belangrijke aanbeveling om bij het moderniseringstraject "een integrale visie te hanteren op de normering van zowel gegevensvergaring als -gebruik: Sv en Wpg moeten in samenhang het opsporingsonderzoek reguleren op een manier die een goede balans biedt tussen effectiviteit en rechtsbescherming".⁵ In 2020 heeft de toenmalige Minister voor Rechtsbescherming in een kamerbrief de noodzaak van vernieuwing van de Wpg en Wjsg uiteengezet.⁶ Ten tijde van het opstellen van de voorstellen voor het nieuwe Wetboek van Strafvordering is hiervan ook uitgegaan. Deze nieuwe gegevensverwerkingswet zou samen met het Wetboek van Strafvordering een coherente regeling moeten gaan vormen voor het verzamelen en verder verwerken van persoonsgegevens in het kader van de strafrechtelijke handhaving van de rechtsorde.

Omdat voor de realisatie en implementatie van deze nieuwe gegevensverwerkingswet geen financiële middelen beschikbaar zijn, hebben de Minister van Justitie en Veiligheid en de toenmalige Minister voor Rechtsbescherming besloten dat deze nieuwe wet er niet komt.⁷ Zij komen daarmee ook terug op de eerder gemaakte meer principiële keuze om de wetgeving zo te ordenen dat de regels voor het verzamelen van

² Kamerstukken II 2022/23, 36 327, nrs. 1-3.

³ Kamerstukken II 2024/25, 36 636, nrs. 1-3.

⁴ Zie Boek 8 inzake internationale en Europese strafrechtelijke samenwerking, voorstel vaststellingswet II.

⁵ Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, 2018, aanbeveling 2.

⁶ Kamerstukken II 2020/21, 32 761, nr. 173.

⁷ Kamerstukken II 2022/23, 36 327, nr. 3, p. 70-71. Zie voorts Kamerstukken II 2021/22, 32 761, nr. 218.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

gegevens ten behoeve van de strafrechtelijke rechtshandhaving in het Wetboek van Strafvordering worden opgenomen en de regels voor de verdere verwerking van die verzamelde gegevens in een afzonderlijke gegevensverwerkingwet. Dit heeft ertoe geleid dat in het voorliggende concept voor een eerste aanvullingswet alsnog enkele bepalingen zijn opgenomen over het bewaren, vernietigen en doelafwijkend gebruiken van persoonsgegevens die zijn verzameld met toepassing van een aantal in het wetboek geregelde opsporingsbevoegdheden.

De AP betreurt het ten zeerste dat de aangekondigde nieuwe gegevensverwerkingwet geen doorgang vindt. Nu daaraan slechts financiële overwegingen ten grondslag liggen, kan de AP niet anders dan concluderen dat de regering kennelijk wel bereid is geld uit te trekken voor de implementatie van het nieuwe wetboek dat onder andere de politie meer bevoegdheden geeft om aanzienlijke hoeveelheden persoonsgegevens te verzamelen, maar niet bereid is te investeren in wetgeving die de verdere verwerking van die gegevens normeert naar de huidige stand van het recht en in een daarbij behorend implementatietraject waarmee de daadwerkelijke naleving van die wetgeving ook wordt gefaciliteerd en verzekerd. Dit acht de AP problematisch omdat - zoals ook verderop uit deze wetgevingstoets blijkt - de normering van bevoegdheden waarmee persoonsgegevens kunnen worden *verzameld* niet los kan worden gezien van de normering van de *verdere verwerking* van die persoonsgegevens. Vraag is bovendien of deze aanpak niet tot onnodige (meer)kosten zal leiden. Voor de implementatie van het nieuwe Wetboek van Strafvordering zullen immers investeringen moeten worden gedaan om IT-systemen aan te passen. Het zou vermoedelijk ook vanuit financieel oogpunt beter zijn om bij die aanpassingen meteen rekening te houden met geactualiseerde en duidelijke regels voor de verwerking van de verzamelde persoonsgegevens (zoals bewaartermijnen, doelbinding, afscherming e.d.).

Gelet op het voorgaande is de AP van oordeel dat de regering alsnog de middelen beschikbaar moet stellen die nodig zijn om de wetgeving voor de (verdere) verwerking van persoonsgegevens die zijn verzameld in het kader van strafrechtelijke rechtshandhaving (en de openbare ordehandhaving) zoals thans opgenomen in de Wpg en Wjsg te herzien en te actualiseren zodat deze aansluit bij het Europese (gegevensbeschermings)recht en de noodzakelijke waarborgen biedt voor de rechten en vrijheden van individuen in een digitale samenleving.

4. Strekking van het voorliggende concept

Het voorliggende concept betreft de eerste aanvullingswet van het nieuwe Wetboek van Strafvordering. In dit concept wordt – zoals hiervoor aangegeven - alsnog een regeling betreffende gegevensverwerking in het nieuwe wetboek opgenomen (artikelen 2.1.18 t/m 2.1.21). Voorts worden enkele nieuwe onderwerpen toegevoegd, wordt invulling gegeven aan gereserveerde onderdelen uit de voorstellen voor de vaststellingswetten, worden omissies in de inmiddels ingediende voorstellen voor de vaststellingswetten hersteld en noodzakelijke wijzigingen en aanvullingen gedaan.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

5. Wetgevingstoets

5.1 Algemeen

Effectieve opsporing, vervolging, berechting en bestraffing van strafbare feiten vormen wezenlijke elementen voor de ordening van onze maatschappij en voor een rechtvaardige en leefbare samenleving.⁸ Maar een rechtvaardige en leefbare samenleving wordt evenzeer gevormd door de bescherming van fundamentele rechten en vrijheden van individuen, waaronder het recht op bescherming van persoonsgegevens. Het is de taak van de wetgever om een wettelijk kader tot stand te brengen dat het mogelijk maakt de verschillende belangen en rechten die moeten worden beschermd met elkaar te verzoenen.⁹

In het nieuwe Wetboek van Strafvordering worden de mogelijkheden om gericht en ongericht grote hoeveelheden persoonsgegevens (heimelijk) te verzamelen substantieel uitgebreid. Gelet op de technologische ontwikkelingen is dit ook begrijpelijk.¹⁰ Maar om deze gegevensverwerkingen in goede banen te leiden en ervoor te zorgen dat deze in overeenstemming zijn met het Unierecht, is duidelijke en nauwkeurige regelgeving noodzakelijk. Regelgeving die de bevoegdheden creëert en inkadert en niet alleen voorziet van waarborgen voor de *inzet* van deze bevoegdheden (zoals in welke gevallen en onder welke voorwaarden een bevoegdheid mag worden ingezet en welke autoriteit daartoe mag beslissen), maar ook van waarborgen voor de *verdere verwerking* (zoals over het analyseren, bewaren, vernietigen en voor een ander doel gebruiken van de verzamelde persoonsgegevens). Om te kunnen beoordelen of de nieuwe regelgeving aan het evenredigheidsbeginsel voldoet, moeten deze waarborgen in samenhang met elkaar kunnen worden beoordeeld.

Tegen deze achtergrond is het zorgwekkend dat de RGR geen enkele keer in de toelichting op de in 2023 en 2024 ingediende voorstellen voor vaststellingswetten I en II wordt genoemd, terwijl de AP in haar eerder uitgebrachte adviezen wel expliciet hiervoor aandacht heeft gevraagd en de lidstaten deze richtlijn sinds 6 mei 2018 moeten toepassen. Ook in de toelichting op het voorliggende concept wordt deze richtlijn slechts één keer genoemd in het kader van de vraag wat onder het begrip 'openbare veiligheid' moet worden verstaan. De AP vindt dit zorgwekkend omdat iedere verwerking van persoonsgegevens raakt aan het fundamentele recht op bescherming van persoonsgegevens. Inmenging in het recht op bescherming van

⁸ Op de overheid rusten ook positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM, waarin rechten zijn gewaarborgd die corresponderen met de in de artikelen 4 en 7 van het Handvest gewaarborgde rechten. Deze positieve verplichtingen impliceren dat materiële en procedurele bepalingen moeten worden vastgesteld en praktische maatregelen moeten worden genomen die het mogelijk maken om criminaliteit gericht tegen personen effectief te bestrijden door middel van doeltreffend onderzoek en doeltreffende vervolging (HvJ EU 6 oktober 2020 C-511/18, C-512/18 en C-520/18 ECLI:EU:C:2020:791 (*La Quadrature du Net*), punt 128).

⁹ HvJ EU 6 oktober 2020 C-511/18, C-512/18 en C-520/18 ECLI:EU:C:2020:791 (*La Quadrature du Net*), punt 127 en 128. Vgl. EHRM 2 december 2008, K.U. tegen Finland, punt 49.

¹⁰ Zie ook overweging 3 van de RGR: "*Snelle technologische ontwikkelingen en de mondialisering brachten nieuwe uitdagingen voor de bescherming van persoonsgegevens. De mate waarin persoonsgegevens worden verzameld en gedeeld, is aanzienlijk gestegen. Dankzij de technologie kunnen bij activiteiten zoals de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen meer dan ooit tevoren persoonsgegevens worden verwerkt.*"



Datum
3 maart 2025

Ons kenmerk
z2024-014439

persoonsgegevens is alleen dan toegestaan indien deze voldoet aan het in artikel 52 van het Handvest opgenomen evenredigheidsbeginsel en de RGR bevat hiervoor belangrijke waarborgen.

In de toelichting op het concept is aangegeven dat de komende jaren *buiten* het kader van het wetgevingsproject nieuw Wetboek van Strafvordering beleid ten aanzien van gegevensverwerking verder zal worden ontwikkeld. De wetgever meent dat Europeesrechtelijke ontwikkelingen eerst moeten worden afgewacht omdat deze nog niet zijn uitgekristalliseerd. Daarnaast wordt gesteld dat verdere normering significante uitvoeringsconsequenties kan meebrengen alsmede een toename van de incidentele uitvoeringskosten van het nieuwe wetboek. Dit zou tot een onwenselijke verlenging van de implementatietermijn van het nieuwe wetboek kunnen leiden.

De AP is van oordeel dat met deze aanpak niet kan worden volstaan. Wanneer de mogelijkheden tot het (ongericht) verzamelen van grote hoeveelheden (gevoelige) persoonsgegevens in het belang van de opsporing worden uitgebreid, dient dit hand in hand te gaan met het versterken van waarborgen met het oog op het recht op bescherming van persoonsgegevens en eerbiediging van de persoonlijke levenssfeer in het belang van het individu. Dit geldt temeer omdat met die digitale opsporingsbevoegdheden de kans alleen maar toeneemt dat onverdachte personen die geen enkele betrokkenheid bij op te sporen strafbare feiten hebben in dergelijke gegevensverzamelingen worden betrokken. Het is daarom van groot belang ervoor te zorgen dat de verwerking van die gegevensverzamelingen in overeenstemming is met het Europese (gegevensbeschermings)recht en aan het evenredigheidsbeginsel voldoet. De AP waarschuwt dat incongruenties tussen nationaal en Europees recht die niet met een (Unierecht)conforme uitlegging kunnen worden gerepareerd, ertoe kunnen leiden dat bepalingen uit het nieuwe Wetboek van Strafvordering in concrete gevallen buiten toepassing moeten blijven. Dit zou ook voor de instanties die met de opsporing en vervolging van strafbare feiten zijn belast een bijzonder onwenselijke situatie van rechtsonzekerheid opleveren en de rechterlijke macht (onnodig) belasten met rechtsvragen op dit vlak.

Ook het projectteam van wetenschappers van vier universiteiten dat de vaste Kamercommissie voor Justitie en Veiligheid ondersteunt en adviseert bij de behandeling van de wetsvoorstellen voor het nieuwe Wetboek van Strafvordering betwijfelt of de afwachtende houding van de regering op dit punt houdbaar is en suggereert dat een meer proactieve koers zou moeten worden gevaren.¹¹

De stelling dat eerst Europeesrechtelijke ontwikkelingen moeten zijn uitgekristalliseerd voordat tot aanpassing van wetgeving wordt overgegaan kan ook om de volgende reden niet worden aanvaard. Dit veronderstelt namelijk dat er in de toekomst met enige zekerheid een moment zal zijn aan te wijzen waarop duidelijk is dat het recht is uitgekristalliseerd. Een dergelijk moment komt waarschijnlijk niet omdat het recht zich altijd ontwikkelt en als het al komt, zal het alleen op een (veel) later moment aan te wijzen zijn. Dat moment afwachten geeft dus veel onzekerheid voor een onbekende, maar mogelijk lange periode waarbij bewust het risico wordt genomen dat de verwerking van persoonsgegevens voor strafvorderlijke doeleinden weliswaar voldoet aan het nieuwe Nederlandse Wetboek van Strafvordering,

¹¹ Project bijstand Tweede Kamer modernisering wetboek van Strafvordering, Inhoudelijks rapportage Boek 2: Het opsporingsonderzoek, Vrije Universiteit, 11 september 2023. Radboud Universiteit, Universiteit Utrecht en Erasmus University Rotterdam, p. 11.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

maar tegelijkertijd in strijd is met het Unierecht. Zoals hiervoor al is opgemerkt kan dit tot zeer ongewenste rechtsonzekerheid leiden.

Aangezien de toelichting op de reeds ingediende voorstellen voor de vaststellingswetten en op het voorliggende concept geen blijk geeft van het feit dat de daarin opgenomen bepalingen zijn getoetst aan het recht op bescherming van persoonsgegevens zoals uitgewerkt in de RGR,¹² is de AP van oordeel dat de Minister van Justitie en Veiligheid en de Staatssecretaris Rechtsbescherming alsnog een nadere analyse moeten uitvoeren om te toetsen of de bepalingen in deze wetsvoorstellen in overeenstemming zijn met de RGR, andere relevante richtlijnen en het Handvest, zoals uitgelegd door het Hof van Justitie en de bepalingen zo nodig (via aanpassing van het voorliggende concept of in een voorstel voor een tweede aanvullingswet) aan te passen. Daarbij dient in ieder geval rekening te worden gehouden met de specifieke punten uit paragraaf 5.3 en 5.4 van deze wetgevingstoets.

5.2 Het Handvest van de grondrechten van de EU en de Richtlijn gegevensbescherming bij rechtshandhaving

5.2.1 Het Handvest van de grondrechten van de Europese Unie

In artikel 8 van het Handvest van de grondrechten van de Europese Unie is het fundamentele recht op bescherming van persoonsgegevens verankerd (*“Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.”*). Het Handvest codificeert belangrijke rechtsbeginselen voor de verwerking van persoonsgegevens (de beginselen van behoorlijkheid, doelbinding en rechtmatigheid) en rechten van betrokkenen (het recht op inzage en rectificatie). Ten slotte bepaalt het Handvest dat een onafhankelijke autoriteit toezicht houdt op de naleving hiervan (in Nederland is dat de AP).

Beperkingen van dit grondrecht zijn op grond van artikel 52 van het Handvest alleen toegestaan wanneer deze bij wet zijn gesteld en voor zover de wezenlijke inhoud van dat recht wordt geëerbiedigd. Het in artikel 52 van het Handvest verankerde evenredigheidsbeginsel brengt voorts met zich dat beperkingen van het recht op bescherming van persoonsgegevens alleen mogen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

Aan de Uniewetgever is de opdracht gegeven om voor alle lidstaten gelijke voorschriften voor de bescherming van persoonsgegevens vast te stellen.¹³ Deze voorschriften zijn opgenomen in de Algemene verordening gegevensbescherming (AVG) en, voor zover het gaat om de verwerking van persoonsgegevens binnen het domein van rechtshandhaving in de Richtlijn gegevensbescherming bij rechtshandhaving (RGR). Met uitzondering van de verwerking van persoonsgegevens in sectoren die zijn uitgezonderd van het toepassingsbereik van deze twee regelingen, bestrijken zij - complementair aan elkaar - iedere verwerking van persoonsgegevens. Beide regelingen geven nadere invulling aan het

¹² Zie ook de grondrechtenparagraaf in de memorie van toelichting bij het voorstel voor vaststellingswet I waarin het accent van de grondrechtentoetsing ligt op toetsing aan het in de Grondwet en het EVRM neergelegde recht op vrijheid, recht op een eerlijke proces en recht op eerbiediging van de persoonlijke levenssfeer, waaronder begrepen het recht op onaantastbaarheid van het lichaam, het huisrecht en het recht op bescherming van het telecommunicatiegeheim. (Kamerstukken II 2022/23, 36 327, nr. 3, p. 61).

¹³ Artikel 16, tweede lid, Verdrag betreffende de werking van Europese Unie.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

grondrecht op bescherming van persoonsgegevens en de eerder genoemde rechtsbeginselen en rechten zoals opgenomen in artikel 8 van het Handvest.

Nu de lidstaten bij de verwerking van persoonsgegevens het Unierecht toepassen, namelijk de AVG respectievelijk de RGR, zijn zij in de context van die verwerking van persoonsgegevens tevens gebonden aan alle in het Handvest gewaarborgde grondrechten en rechtsbeginselen. Artikel 51, eerste lid, van het Handvest bepaalt immers dat het Handvest van toepassing op de lidstaten wanneer zij het recht van de Unie ten uitvoer brengen.

Het Unierecht is in toenemende mate doorgedrongen in het van oorsprong nationale strafprocesrecht. Voorbeelden hiervan zijn de diverse richtlijnen in verband met het versterken van de rechten van de verdediging¹⁴ en richtlijnen of verordeningen met betrekking tot de strafrechtelijke samenwerking tussen de lidstaten.¹⁵ Zoals uit de volgende paragraaf blijkt, heeft de Richtlijn gegevensbescherming bij rechtshandhaving tot gevolg dat ook dat deel van het strafprocesrecht dat bestaat uit het verzamelen, analyseren en verder verwerken van persoonsgegevens met het oog op het onderzoek, de opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen wordt beheerst door het Unierecht en daarom in overeenstemming moet zijn met alle in het Handvest verankerde grondrechten.

5.2.2 De Richtlijn gegevensbescherming bij rechtshandhaving

Voor de volledigheid gaat deze paragraaf kort in op het toepassingsbereik van de RGR. Van belang hierbij is dat - anders dan het toepassingsbereik van Kaderbesluit 2008/997 dat door de RGR is vervangen¹⁶ - de RGR zich niet slechts beperkt tot de bescherming van persoonsgegevens bij de uitwisseling van persoonsgegevens tussen de lidstaten en Europese organen, maar kort gezegd van toepassing is op iedere vorm van verzamelen, bewaren, gebruiken en verstrekken van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten, de tenuitvoerlegging van straffen en de handhaving van de openbare orde. De richtlijn is namelijk van toepassing wanneer aan de volgende, cumulatieve voorwaarden is voldaan.

a. Er is sprake van geautomatiseerde verwerking van persoonsgegevens of van verwerking van persoonsgegevens die bedoeld zijn om in een bestand te worden opgenomen

Onder het begrip persoonsgegevens wordt verstaan alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.¹⁷ Het moet gaan om persoonsgegevens die geheel of gedeeltelijk geautomatiseerd worden verwerkt. Dit betekent dat elke digitale verwerking van persoonsgegevens hieronder valt. Maar ook persoonsgegevens die niet-geautomatiseerd worden verwerkt vallen onder de reikwijdte van de RGR indien deze bedoeld zijn om in een bestand, zoals bijvoorbeeld in het dossier van een opsporingsonderzoek, te worden opgenomen.¹⁸

¹⁴ Enkele voorbeelden zijn Richtlijn 2010/64 inzake het recht op vertolking en vertaling in strafprocedures; Richtlijn 2012/13 inzake het recht op informatie in strafprocedures; Richtlijn 2013/48 inzake het recht op toegang tot een advocaat in strafprocedures.

¹⁵ Enkele voorbeelden zijn Richtlijn 2014/41 betreffende het Europees onderzoeksbevel in strafzaken en Verordening 2018/ inzake wederzijdse erkenning van bevestigingsbevelen en confiscatiebevelen.

¹⁶ Zie artikel 1, tweede lid, onderdeel a t/m c, van Kaderbesluit 2008/997.

¹⁷ Artikel 1, onder 1, RGR.

¹⁸ Artikel 2, tweede lid, RGR.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

Van belang is voorts te onderstrepen dat onder het verwerken in de zin van de RGR ook handelingen vallen die bestaan uit het verzamelen – in de context van strafvordering veelal aangeduid als vergaren - van dergelijke persoonsgegevens.¹⁹ Het Hof van Justitie bevestigt dit ook in zijn jurisprudentie.²⁰ Uit de wettelijke definitie en de rechtspraak blijkt dat het begrip ‘verwerking’ een bijzonder ruime betekenis heeft.²¹ De toepasselijkheid van de RGR start dus niet pas bij het *verder* verwerken van reeds verzamelde of vergaarde persoonsgegevens, maar moet ook in acht worden genomen bij het verzamelen van persoonsgegevens voor de doelen van de RGR.

b. De verwerking vindt plaats met het oog op voorkoming, onderzoek, opsporing en vervolging van strafbare feiten, tenuitvoerlegging van straffen of openbare ordehandhaving

De verwerking van persoonsgegevens komt binnen de beschermende werking van de RGR te vallen wanneer die verwerking geschiedt met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Ook valt een verwerking binnen de reikwijdte van de RGR indien deze geschiedt met het oog op de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.²² Dit laatste wordt in de Nederlandse context veelal aangeduid als de handhaving van de openbare orde. Het behoeft geen betoog dat het verzamelen van persoonsgegevens in het kader van het opsporingsonderzoek geschiedt met het oog op het onderzoek, de opsporing en de vervolging van strafbare feiten. Maar ook bijvoorbeeld de verstrekking van onder de richtlijn verzamelde persoonsgegevens en de verwerking van persoonsgegevens met het oog op de tenuitvoerlegging van straffen en maatregelen valt binnen het bereik van de richtlijn.

c. De verwerking geschiedt door een bevoegde autoriteit

Ten slotte geldt dat de verwerking geschiedt door een bevoegde autoriteit.²³ Onder bevoegde autoriteit wordt in de RGR onder andere verstaan iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.²⁴ De opsporingsambtenaar, officier van justitie en rechter-commissaris kwalificeren als bevoegde autoriteit in de zin van de RGR.

De bij sommigen levende gedachte dat de RGR slechts betekenis heeft voor datgene wat is geregeld in de Wpg en Wjsg, moet op grond van het voorgaande dan ook als onjuist worden bestempeld. De RGR strekt zich onder andere ook uit tot belangrijke delen van het Wetboek van Strafvordering, waaronder de

¹⁹ Artikel 1, onder 2, RGR.

²⁰ HvJEU 30 januari 2024, C-118/21 (*NG*), r.o. 41 en 42 en HvJEU 4 oktober 2024, C-548/21, ECLI:EU:C:2024:830 (*Landeck*), r.o. 79 en 80. Zie ook HvJEU 26 januari 2023, C-205/21, ECLI:EU:C:2023:49 (*Ministerstvo na vatreshnite raboti*) over het verzamelen van biometrische en genetische gegevens in het kader van een strafprocedure.

²¹ Zie artikel 3, onder 2, RGR.

²² Artikel 1, eerste lid, RGR.

²³ Artikel 1, eerste lid, RGR.

²⁴ Artikel 3, onder 7, RGR. Daarnaast wordt onder ‘bevoegde autoriteit’ ook verstaan: ieder ander orgaan dat of iedere andere entiteit die krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

bepalingen in Boek 2 betreffende het opsporingsonderzoek die zien op het verzamelen of verder verwerken van persoonsgegevens.²⁵ Deze bepalingen dienen dan ook in overeenstemming te zijn met de RGR en de relevante rechtspraak van het Hof van Justitie van de Europese Unie.

5.3 Relevante rechtspraak van het Hof van Justitie

De rechtspraak van het Hof van Justitie laat zien dat het Europese gegevensbeschermingsrecht in toenemende mate van invloed is op het nationale strafprocesrecht. Het gaat hierbij niet alleen om uitleg die het Hof van Justitie geeft aan de RGR, maar ook over andere richtlijnen, zoals Richtlijn 2002/58 (e-Privacy)²⁶ en Richtlijn 2016/681 (PNR-gegevens),²⁷ gelezen in samenhang met de artikelen 7 en 8 van het Handvest voor de grondrechten van de Europese Unie.

5.3.1 Bevel tot verstrekking van (persoons)gegevens

Uit de rechtspraak van het Hof van Justitie met betrekking tot Richtlijn 2002/58 (e-Privacy) en Richtlijn 2016/681 (PNR-gegevens) gelezen in samenhang met onder andere het in artikel 52 van het Handvest neergelegde evenredigheidsbeginsel, is duidelijk geworden dat voorafgaande toetsing door een rechter of onafhankelijke bestuurlijke autoriteit in ieder geval is vereist wanneer sprake is van een bevel tot verstrekking van (a) verkeers- en locatiegegevens bij aanbieders van communicatiediensten²⁸ en (b) passagiersgegevens bij de passagiersinformatie-eenheid.²⁹ Met betrekking tot deze voorafgaande toetsing heeft het Hof van Justitie voorts bepaald dat de instantie die belast is met die voorafgaande toetsing enerzijds niet betrokken mag zijn bij de uitvoering van het betrokken strafrechtelijk onderzoek en anderzijds neutraal moet zijn ten opzichte van de partijen in de strafprocedure. Dat is, aldus het Hof, niet het geval bij een openbaar ministerie dat de onderzoeksprocedure leidt en, in voorkomend geval, optreedt als openbaar aanklager.³⁰ Hieruit volgt dat de officier van justitie niet als onafhankelijke bestuurlijke autoriteit kan worden aangemerkt.³¹

De eis van voorafgaande toestemming door een rechter of onafhankelijke bestuurlijke autoriteit die het Hof van Justitie stelt houdt nauw verband met het feit dat op basis van de betrokken gegevens nauwkeurige conclusies kunnen worden getrokken met betrekking tot de persoonlijke levenssfeer van

²⁵ Zie ook K.C. van Horssen, *Aan het uitkristalliseren: de betekenis van het EU-recht voor opsporingsbevoegdheden*, Tijdschrift voor Bijzonder Strafrecht en Handhaving, 2024, p. 22-32.

²⁶ Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).

²⁷ Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit.

²⁸ Zie o.a. HvJEU 2 maart 2021 C-746/18 ECLI:EU:C:2021:152 (*Prokuratuur*) en HvJEU 5 april 2022 C-140/20 ECLI:EU:C:2022:258 (*Commissioner of An Garda Síochána*).

²⁹ HvJEU 21 juni 2022 C-817/19, ECLI:EU:C:2022:491 (*Ligue des droits humains*), punt 223 en 224.

³⁰ HvJEU 2 maart 2021 C-746/18 ECLI:EU:C:2021:152 (*Prokuratuur*), punt 54-55.

³¹ HvJEU 2 maart 2021 C-746/18 ECLI:EU:C:2021:152 (*Prokuratuur*), punt 59; HvJEU 5 april 2022 C-140/20 ECLI:EU:C:2022:258 (*Commissioner of An Garda Síochána*), punt 107 en 108; HvJEU 21 juni 2022 C-817/19, ECLI:EU:C:2022:491 (*Ligue des droits humains*), punt 225, 226 en 244.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

betrokkene(n)³² of, in het geval van PNR-gegevens, dat de betrokken gegevens, hoewel deze op zichzelf beschouwd geen nauwkeurige informatie over het privéleven van een betrokkene verschaffen, samen beschouwd wel inzicht verschaffen over bepaalde delen van het privéleven van de betrokkene, zoals bijvoorbeeld reisroutes en reisgewoontes, relaties tussen personen, voedingsgewoonten en informatie over de financiële situatie van betrokkene.³³

Daarnaast volgt uit de rechtspraak van het Hof dat de toegang tot verkeers- en locatiegegevens alleen dan voldoet aan het evenredigheidsbeginsel indien dit is beperkt tot procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid.³⁴ Wat betreft passagiersgegevens volgt uit de PNR-richtlijn zelf dat de toegang tot deze gegevens slechts is toegestaan voor procedures ter bestrijding van terroristische misdrijven en ernstige criminaliteit.³⁵

In vervolg op de rechtspraak van het Hof van Justitie met betrekking tot verkeers- en locatiegegevens heeft de Hoge Raad in zijn arrest van 5 april 2022 bepaald dat voor een vordering/bevel tot verstrekking van deze gegevens een machtiging van de rechter-commissaris is vereist.³⁶ In lijn met deze uitspraak is de AP van oordeel dat voor een bevel tot verstrekking van passagiersgegevens eveneens een machtiging van de rechter-commissaris is vereist. Op basis van de hierboven aangehaalde rechtspraak van het Hof van Justitie kan dit in beginsel ook een onafhankelijke bestuurlijke autoriteit zijn, maar in ieder geval niet een officier van justitie, ook niet als deze op afstand staat van het opsporingsonderzoek in welk kader de verstrekking van de gegevens wordt bevolen.

De AP constateert dat het voorliggende concept dat onder andere wijzigingen van de bepalingen uit de reeds ingediende voorstellen voor de vaststellingswetten I en II bevat, geen wijziging voorstelt van de artikelen betreffende de verstrekking van gegevens ten behoeve van het onderzoek (artikel 2.7.44 e.v.) in het voorstel voor vaststellingswet I. Gelet op de hierboven aangehaalde jurisprudentie had dit wel in de rede gelegen.

Hierbij wijst de AP op het feit dat het vereiste van een voorafgaande machtiging van de rechter-commissaris geen vrijblijvend karakter heeft. Uitwerking van dit vereiste in de vorm van een algemene (vangnet)bepaling die de officier van justitie de optie geeft om voor de inzet van een bepaalde bevoegdheid de rechter-commissaris om een machtiging te vragen (artikel 2.1.7) volstaat dan ook niet als waarborg voor strafvorderlijk handelen in overeenstemming met het Unierecht.

Daarnaast merkt de AP op dat het voor de hand ligt in ieder geval na te gaan welke andere categorieën van persoonsgegevens gelijk gesteld moeten worden met verkeers- en locatiegegevens en PNR-gegevens omdat daaruit eveneens nauwkeurige conclusies over (onderdelen van) het privéleven van een betrokkene kunnen worden getrokken. Voor dergelijke vergelijkbare categorieën van persoonsgegevens ligt

³² HvJEU 2 maart 2021 C-746/18 ECLI:EU:C:2021:152 (*Prokuratuur*), punt 39; HvJEU 5 april 2022 C-140/20 ECLI:EU:C:2022:258 (*Commissioner of An Garda Síochána*), punt 45.

³³ HvJEU 21 juni 2022 C-817/19, ECLI:EU:C:2022:491 (*Ligue des droits humains*), punt 100.

³⁴ HvJEU 2 maart 2021 C-746/18 ECLI:EU:C:2021:152 (*Prokuratuur*), punt 45.

³⁵ Artikel 1, tweede lid, Richtlijn 2016/681.

³⁶ HR 5 april 2022, ECLI:NL:HR:2022:475, r.o. 6.11.4.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

logischerwijs een vergelijkbare regeling met voorafgaande machtiging van de rechter-commissaris of een onafhankelijke bestuurlijke autoriteit in de rede.³⁷ De AP denkt hierbij in ieder geval aan een bevel tot verstrekking van gegevens gericht tot banken en andere financiële instellingen voor zover het hierbij niet slechts gaat om gegevens betreffende de tenaamstelling van een bankrekeningnummer en NAW-gegevens van de rekeninghouder. Op basis van transactiegegevens kunnen immers (zeer) nauwkeurige conclusies over het privéleven van de desbetreffende rekeninghouder worden getrokken. Voor zover aannemelijk is dat de te verstrekken transactiegegevens bijzondere persoonsgegevens als bedoeld in artikel 10 van de RGR omvatten, zal in elk geval een machtiging van de rechter-commissaris zijn vereist overeenkomstig artikel 2.7.46, derde lid, in het voorstel voor vaststellingswet I. Voorts is de AP van oordeel dat voor de verstrekking van met ANPR-camera's vastgelegde kentekengegevens, een voorafgaande machtiging van de rechter-commissaris voor de hand ligt (zie ook paragraaf 5.4.4).

5.3.2 Onderzoek aan digitale gegevensdragers of geautomatiseerde werken

In de Landeck-uitspraak van 4 oktober 2024 heeft het Hof van Justitie nadere uitleg gegeven aan de RGR in relatie tot het verkrijgen van toegang tot op een (inbeslaggenomen) mobiele telefoon opgeslagen gegevens.³⁸ Het is geen verrassing meer dat de inhoud van een mobiele telefoon zéér veel (gevoelige) informatie over het privéleven van de gebruiker ervan kan prijsgeven. In lijn met de hiervoor besproken rechtspraak, heeft het Hof van Justitie bepaald dat voor het onderzoek aan een mobiele telefoon teneinde toegang te krijgen tot de daarop opgeslagen gegevens ten behoeve van de opsporing eveneens een voorafgaande toetsing door een rechter of onafhankelijk bestuursorgaan is vereist. Toegang tot de op een mobiele telefoon opgeslagen gegevens, zoals verkeer- en locatiegegevens, foto's, browsergeschiedenis en communicatie, maar mogelijk ook bijzondere persoonsgegevens zoals gegevens betreffende politieke of religieuze opvattingen of betreffende de gezondheid, maakt het immers mogelijk om zeer nauwkeurige conclusies te trekken over het privéleven van de betrokkene. De inmenging in de door de artikel 7 en 8 van het Handvest gewaarborgde grondrechten moet dan ook volgens het Hof worden aangemerkt als 'ernstig of zelfs bijzonder ernstig'. Alleen al het risico van een ernstige of zelfs zeer ernstige inmenging in de grondrechten van betrokkenen' dat gepaard gaat met de toegang tot gegevens op een mobiele telefoon maakt volgens het Hof dat de voorafgaande toetsing door een rechter of onafhankelijk bestuursorgaan is vereist.³⁹ Vergelijk ook hetgeen het Hof stelt ten aanzien van de voorafgaande toetsing bij het vorderen van verkeers- en locatiegegevens in het Prokuratuur-arrest: "*De beoordeling van de ernst van de inmenging die de toegang voor de persoonlijke levenssfeer van de betrokken personen met zich brengt, gebeurt [...] noodzakelijkerwijs aan de hand van het algemene risico dat verband houdt met de categorie van de gevraagde gegevens, waarbij het overigens niet van belang is of de daaruit voortvloeiende informatie betreffende de persoonlijke levenssfeer al dan niet concreet gevoelig is.*" (onderstreping AP).⁴⁰

³⁷ Zie ook punt 14 in de noot van R. Te Molder bij HvJEU 5 april 2022, C-140/20 (Commissioner of the Garda Síochána e.a.) in EHRC Updates.

³⁸ HvJEU 4 oktober 2024, C-548/21, ECLI:EU:C:2024:830 (*Landeck*).

³⁹ HvJEU 4 oktober 2024, C-548/21, ECLI:EU:C:2024:830 (*Landeck*), punt 92 t/m 95 en 102.

⁴⁰ HvJEU 2 maart 2021 C-746/18 ECLI:EU:C:2021:152 (*Prokuratuur*), punt 40.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

Bij gebrek aan een specifieke wettelijke regeling, heeft de Hoge Raad sinds 2017 een beoordelingskader ontwikkeld met betrekking tot het onderzoek aan een inbeslaggenomen smartphone.⁴¹ De Hoge Raad maakt daarin onderscheid tussen onderzoek dat zo verstrekkend is dat een min of meer compleet beeld van bepaalde aspecten van het persoonlijke leven van de betrokkene wordt verkregen en onderzoek dat slechts een beperkte inbreuk op de persoonlijke levenssfeer oplevert en verbindt hieraan - onder verwijzing naar artikel 8 EVRM - verschillende conclusies wat betreft de autoriteit die dat onderzoek rechtmatig kan uitvoeren. Uit de hiervoor besproken Landeck-uitspraak blijkt dat bij de beoordeling van de rechtmatigheid van het onderzoek aan op een smartphone (of andere digitale-gegevensdrager of geautomatiseerd werk) opgeslagen gegevens, niet langer alleen rekening moet worden gehouden met het recht op eerbiediging van de persoonlijke levenssfeer zoals verankerd in artikel 8 EVRM en artikel 7 Handvest, maar ook met het recht op bescherming van persoonsgegevens zoals neergelegd in artikel 8 Handvest en onder andere uitgewerkt in de RGR. Tegen deze achtergrond zal naar het oordeel van de AP het door de Hoge Raad ontwikkelde beoordelingskader aanpassing behoeven. In de Nederlandse rechtspraak lijkt deze gedachte ook al post te vatten.⁴²

Het voorgaande betekent ook dat de in het voorstel voor vaststellingswet I voorgestelde regeling voor het stelselmatig respectievelijk ingrijpend stelselmatig onderzoek van gegevens in een digitale-gegevensdrager of geautomatiseerd werk (artikel 2.7.38) evenmin in stand kan blijven. Daarbij komt dat uit de uitspraak van het Hof van Justitie volgt dat de wet voldoende nauwkeurig moet omschrijven bij verdenking van welk soort strafbare feiten dergelijk onderzoek kan worden verricht waarbij bovendien het evenredigheidsbeginsel moet worden gewaarborgd.⁴³ Het voorgestelde artikel 2.7.38 in zijn huidige vorm stelt geen nadere voorwaarden wat betreft de ernst van het strafbare feit in welk geval het daar bedoelde onderzoek kan plaatsvinden, terwijl het Wetboek van Strafvordering zeer ruime bevoegdheden tot inbeslagneming kent.

Ten slotte wijst de AP in dit verband nog op het volgende. In het voorstel voor vaststellingswet I is de bevoegdheid uit het huidige wetboek overgenomen dat een opsporingsambtenaar bij staandehouding of aanhouding, ter vaststelling van de identiteit de verdachte, de verdachte aan zijn kleding kan onderzoeken en de voorwerpen kan onderzoeken die hij met zich voert.⁴⁴ In het concept wordt deze bepaling zodanig aangepast dat een aangehouden verdachte kan worden onderzocht aan kleding en meegevoerde voorwerpen zonder dat gespecificeerd is met welk doel dit onderzoek kan plaatsvinden. Los van het feit dat de AP van oordeel is dat het doel van dit onderzoek in de wet moet zijn gespecificeerd, wijst de AP er vooral op dat dit onderzoek aan meegevoerde voorwerpen - gelet op hiervoor toegelichte Landeck-uitspraak - niet kan bestaan uit het kijken in en onderzoeken van gegevens op een meegevoerde (of bij een

⁴¹ HR 4 april 2017, ECLI:NL:HR:2017:584; HR 9 juli 2019, ECLI:NL:HR:2019:1079.

⁴² Gerechtshof Den Haag 22 januari 2025, ECLI:NL:GHDHA:2025:66, onder Bespreking verweer omtrent vormverzuim ex artikel 359a van het WvSv: "Tegen deze achtergrond is het hofthans van oordeel dat het eerder aangehaalde beoordelingskader bijstelling behoeft in die zin dat het er inmiddels voor gehouden moet worden dat niet alleen het kennisnemen van gegevens, maar ook handelingen teneinde gegevens voor kennisneming beschikbaar te maken, indien sprake is van een risico van een ernstige of zelfs zeer ernstige inmenging in de grondrechten van de betrokkene slechts mag respectievelijk mogen plaatsvinden na een voorafgaande toetsing door een rechter of een onafhankelijk bestuursorgaan."

⁴³ HvJEU 4 oktober 2024, C-548/21, ECLI:EU:C:2024:830 (Landeck), punt 110.

⁴⁴ Artikel 55b Sv en artikel 2.6.6, voorstel voor vaststellingswet I.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

insluitingsfouilleren) mobiele telefoon of vergelijkbaar apparaat, ook niet als dit onderzoek zich beperkt tot het vaststellen van de identiteit van de staandegehouden of aangehouden verdachte.⁴⁵ Dit dient in de toelichting tot uitdrukking te worden gebracht.

5.3.3 Stelselmatige afname en opslag van vingerafdrukken, biometrische gezichtsopnamen en DNA-gegevens
Een andere uitspraak van het Hof van Justitie die van belang is voor de regeling in het Wetboek van Strafvordering betreft de uitspraak 26 januari 2023 betreffende verzameling van fotografische en vingerafdrukgegevens met het oog op de registratie daarvan en afname van biologische monsters met het oog op het aanmaken van een DNA-profiel.⁴⁶ Ook de uitspraak van het Hof van Justitie van 30 januari 2024 gaat in op de verwerking en opslag van biometrische en genetische gegevens.⁴⁷

Op grond van artikel 10 van de RGR is de verwerking van dergelijke bijzondere persoonsgegevens slechts toegestaan indien de verwerking 'strikt noodzakelijk' is en voor de verwerking ervan een expliciete wettelijke grondslag bestaat. In de hierboven genoemde uitspraak heeft het Hof aangegeven dat een wettelijke regeling die voorziet in het stelselmatig verzamelen van biometrische en/of genetische gegevens van iedere persoon die verdacht wordt van een opzettelijk gepleegd misdrijf dat ambtshalve vervolgbaar is, in beginsel in strijd is met het vereiste uit artikel 10 van de Richtlijn dat de verwerking van dergelijke persoonsgegevens alleen is toegestaan als dit strikt noodzakelijk is. Zo'n verwerking kan er immers toe leiden dat op algemene en ongedifferentieerde wijze biometrische en/of genetische gegevens van de meeste verdachten worden verzameld aangezien het criterium van een ambtshalve vervolgbaar en opzettelijk gepleegd strafbaar feit bijzonder algemeen is en van toepassing kan zijn op een groot aantal strafbare feiten ongeacht de aard en de ernst ervan.⁴⁸ Het enkele feit dat een persoon verdacht wordt van een dergelijke strafbaar feit, kan volgens het Hof niet de aanname rechtvaardigen dat verzamelen van de bedoelde persoonsgegevens strikt noodzakelijk is. Er kunnen immers gevallen zijn waarin het verzamelen van die gegevens niet specifiek noodzakelijk is voor het lopende onderzoek naar het strafbare feit waar de betrokkene van verdacht wordt. Of de verzameling strikt noodzakelijk is in het kader van andere procedures dan het lopende onderzoek waarin de betrokkene verdachte is, kan volgens het Hof slechts worden bepaald aan de hand van alle relevante factoren, zoals de aard en de ernst van het strafbare feit waarvan de betrokkene wordt verdacht, de bijzondere omstandigheden van dat strafbare feit, het mogelijk verband van dat strafbare feit met andere lopende procedures en de antecedenten en het persoonlijke profiel van de verdachte.⁴⁹ Wanneer de wettelijke regeling tot het verzamelen van deze gegevens niet voorziet in het vereiste dat wordt nagegaan of de gegevensverzameling strikt noodzakelijk is voor de verwezenlijking van de nagestreefde specifieke doelstellingen, is deze regeling in strijd met het Unierecht en de RGR in het bijzonder.

⁴⁵ Vgl. ABRvS 3 april 2024, ECLI:NL:RVS:2024:1387, r.o. 9.3 waaruit blijkt dat artikel 59, achtste lid, Vw 2000 geen toereikende wettelijke grondslag biedt voor het onderzoek van een mobiele telefoon van een vreemdeling.

⁴⁶ HvJEU 26 januari 2023, C-205/21 ECLI:EU:C:2023:49 (*Ministerstvo na vatreshnite raboti*)

⁴⁷ HvJEU 30 januari 2024, C-118/22 ECLI:EU:C:2024:97 (NG).

⁴⁸ HvJEU 26 januari 2023, C-205/21 ECLI:EU:C:2023:49 (*Ministerstvo na vatreshnite raboti*), punt 129 en HvJEU 30 januari 2024, C-118/22 ECLI:EU:C:2024:97 (NG), punt 64-65.

⁴⁹ HvJEU 26 januari 2023, C-205/21 ECLI:EU:C:2023:49 (*Ministerstvo na vatreshnite raboti*), punt 132 en HvJEU 30 januari 2024, C-118/22 ECLI:EU:C:2024:97 (NG), punt 67.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

In het licht van deze uitspraak, is de AP van oordeel dat de regeling in het Wetboek van Strafvordering (huidige artikel 55c, vierde lid, Sv) die in het concept is overgenomen⁵⁰ om de hierna volgende redenen niet langer houdbaar is. Deze regeling heeft dus aanpassing teneinde verenigbaarheid met het Unierecht te verzekeren.

Artikel 2.6.9, tweede lid, in het voorstel voor vaststellingswet I bevat een regeling voor het afnemen van gezichtsopnamen en vingerafdrukken van iedere verdachte die is aangehouden of wordt verhoord voor een strafbaar feit waarop een gevangenisstraf van vier jaar of meer is gesteld. Indien de verdachte is aangehouden of wordt verhoord voor een ander strafbaar feit, dan kunnen gezichtsopnamen en vingerafdrukken worden afgenomen als twijfel over zijn identiteit bestaat (artikel 2.6.9, derde lid). Indien bij staandehouding twijfel over de identiteit van een verdachte bestaat, kunnen van hem eveneens vingerafdrukken worden afgenomen (artikel 2.6.9, eerste lid). Doel van de verwerking van deze persoonsgegevens is om een juiste, betrouwbare en zorgvuldige vaststelling van de identiteit van verdachten en veroordeelden *in de strafrechtssketen* te waarborgen en identiteitsfraude tegen te gaan.⁵¹ De afgenomen vingerafdrukken en gezichtsopnamen worden vastgelegd in de strafrechtssketendatabank. Bij aanhouding, verhoor en staandehouding kan worden geverifieerd of de persoon in kwestie al bekend is bij justitie, dat wil zeggen of zijn gegevens (vingerafdrukken en identiteitsgegevens) al eerder in de strafrechtssketendatabank zijn opgenomen. Bij vervolcontacten met de autoriteiten in de strafrechtssketen, kunnen deze autoriteiten de door de verdachte opgegeven identiteit controleren aan de hand van de in de strafrechtssketendatabank vastgelegde identiteitsgegevens.

Het in het voorliggende concept voorgestelde zesde lid van artikel 2.6.9 bepaalt dat gezichtsopnamen en vingerafdrukken die van een verdachte zijn afgenomen met het oog op de identiteitsvaststelling in de strafrechtssketen 'kunnen worden verwerkt voor het voorkomen, opsporen, vervolgen en berechten van strafbare feiten en het vaststellen van de identiteit van een overleden persoon'. Dit betreft een omzetting van het huidige artikel 55c, vierde lid, in het nieuwe wetboek. Het gaat hierbij dus om het gebruik van de afgenomen vingerafdrukken en gezichtsopnamen voor *een ander doel* dan het doel waarvoor zij zijn verzameld.

In het Besluit identiteitsvaststelling verdachten en veroordeelden (hierna: Bivv) is een regeling uitgewerkt voor het bewaren van de afgenomen vingerafdrukken niet alleen in de strafrechtssketendatabank, maar tevens ook in een databank voor opsporingsdoeleinden. Uit de toelichting op het Bivv blijkt dat de van de verdachte afgenomen vingerafdrukken gelijktijdig worden gezonden naar de strafrechtssketendatabank⁵² én naar de politiedatabank HAVANK ten behoeve van de opsporing van strafbare feiten.⁵³ Hoewel het Bivv hierover niets regelt, blijkt uit kamerstukken dat eenzelfde procedure wordt gevolgd voor de gezichtsopnamen die van verdachten worden gemaakt. Ook deze worden gelijktijdig en automatisch naar

⁵⁰ Zie voorgestelde zesde lid van artikel 2.6.9.

⁵¹ Kamerstukken II 2007/08, 31 436, nr. 5, p. 1 en 2.

⁵² Meer specifiek naar de onder het beheer van de Justitiële Informatiedienst vallende en aan de strafrechtssketendatabank gekoppelde biometrievoorziening.

⁵³ Stb. 2016, 117, p. 11.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

de Justitiële informatiedienst én naar de relevante politiesystemen (HAVANK/Catch) gezonden.⁵⁴ Deze vingerafdrukken en gezichtsopnamen worden bewaard en gebruikt voor de opsporing van (toekomstige) strafbare feiten. Zie ook hierna paragraaf 5.4.3 over het opnemen en bewaren van bijzondere persoonsgegevens in databanken.

Nu het voorgestelde artikel 2.6.9, zesde lid, inhoudelijk ongewijzigd is overgenomen uit het huidige artikel 55c, vierde lid, is kennelijk geen wijziging in deze gang van zaken voorzien. De AP merkt op dat in deze regeling een afweging of de verwerking van de biometrische gegevens 'strikt noodzakelijk' is ontbreekt. Er wordt immers geen rekening gehouden met de aard en de ernst van het strafbare feit waarvan de verdachte wordt verdacht, de bijzondere omstandigheden van dat strafbare feit, het mogelijk verband van dat strafbare feit met andere lopende procedures en de antecedenten en het persoonlijke profiel van de verdachte. De regeling leidt er namelijk toe dat van iedere verdachte die wordt aangehouden of verhoord voor een strafbaar feit waarop een gevangenisstraf van vier jaar of meer is gesteld⁵⁵ en ongeacht de concrete omstandigheden van het geval of de persoon van de verdachte, gezichtsopnamen en vingerafdrukken worden afgenomen en in de databank bij de politie worden opgeslagen voor toekomstig gebruik, dus zonder in het concrete geval vast te stellen of deze verwerking strikt noodzakelijk is. Hetzelfde geldt voor de vingerafdrukken en gezichtsopnamen die bij twijfel over de identiteit van een verdachte bij staandehouding, aanhouding of verhoor worden afgenomen. Ook hiervoor geldt dat zij zonder beoordeling van de strikte noodzakelijkheid in de databank bij de politie belanden.

Daarnaast geldt dat uit eerdergenoemde uitspraak van het Hof van Justitie ook volgt dat het vereiste van artikel 10 van de RGR dat de verwerking van bijzondere persoonsgegevens (waaronder biometrische en genetische gegevens) moet zijn toegestaan bij lidstatelijke recht met zich meebrengt dat de toepasselijke bepalingen een voldoende duidelijke en nauwkeurige rechtsgrondslag moeten bevatten.⁵⁶ De toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze bepalingen van toepassing zijn, zoals vereist door de rechtspraak van het Hof van Justitie en het Europees Hof voor de Rechten van de Mens.⁵⁷ Dit betekent volgens het Hof dat er geen onduidelijkheid mag bestaan over de voorwaarden die gelden voor de verwerking van biometrische en genetische gegevens. Zowel de betrokkene als de bevoegde autoriteiten moeten immers nauwkeurig kunnen bepalen onder welke voorwaarden die verwerking kan plaatsvinden en voor welke doelen die verwerking rechtmatig kan worden verricht.⁵⁸

⁵⁴ Aanhangsel Handelingen II vergaderjaar 2018/19, nr. 3932 (Beantwoording vragen van het lid Verhoeven door de Minister van Justitie en Veiligheid d.d. 11 september 2019), antwoorden 2 en 4. Zie voorts bijv. ook Aanhangsel Handelingen II vergaderjaar 2024/25, nr. 770 (Beantwoorden vragen van leden van de Kamer door de Minister van Veiligheid en Justitie d.d. 9 december 2024), antwoord 23.

⁵⁵ Met inbegrip van de ruim zestig overige lichtere strafbare feiten die in artikel 2.1.8 gelijk zijn gesteld aan een strafbaar feit waarop een gevangenisstraf van vier jaar of meer is gesteld.

⁵⁶ Het Hof maakt hierbij ook onderscheid tussen de bepaling ter omzetting van artikel 10 van RGR (vgl. in NL artikel 5 Wpg) en de bepalingen krachtens welke een verwerking van bijzondere persoonsgegevens kan zijn toegestaan. Zie HvJEU 26 januari 2023, C-205/21, ECLI:EU:C:2023:49 (*Ministerstvo na vatreshnite raboti*), punt 68.

⁵⁷ Zie ook overweging 33 RGR waarin voorts is bepaald dat in het lidstatelijke recht dat de verwerking van persoonsgegevens binnen het toepassingsgebied van deze richtlijn regelt, ten minste de doeleinden, de te verwerken persoonsgegevens en de doeleinden van de verwerking dienen te worden gespecificeerd, alsmede de procedures voor het waarborgen van de integriteit en vertrouwelijkheid van persoonsgegevens en de procedures voor de vernietiging ervan.

⁵⁸ HvJEU 26 januari 2023, C-205/21, ECLI:EU:C:2023:49 (*Ministerstvo na vatreshnite raboti*), punt 65 en 66.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

Naast het feit dat de hiervoor besproken stelselmatige *verzameling* en *opslag* in een databank van vingerafdrukken en gezichtsopnamen ten behoeve van opsporing van (toekomstige) strafbare feiten niet voldoet aan de eis van strikte noodzakelijkheid, geldt daarnaast dat ook de regeling voor het *gebruik* van dergelijke biometrische gegevens niet voldoet aan de eisen die het Unierecht daaraan stelt. Er zijn immers geen voorwaarden gesteld aan het gebruik (bijv. raadplegen door middel van het geautomatiseerd vergelijken) van de in de databank opgeslagen gezichtsopnamen en vingerafdrukken met gezichtsopnamen of vingerafdrukken die in het kader van een opsporingsonderzoek zijn veiliggesteld.⁵⁹ Zo is niet duidelijk voor welk soort strafbare feiten de databank kan worden geraadpleegd en welke autoriteit hiertoe kan beslissen.

Al het voorgaande leidt ertoe dat de AP van oordeel is dat de regeling van het afnemen, opslaan en gebruiken van gezichtsopnamen en vingerafdrukken ten behoeve van de opsporing moet worden aangepast om deze in overeenstemming te brengen met het Unierecht.

5.4 Verwerking van verzamelde persoonsgegevens

De voorstellen voor het nieuwe Wetboek van Strafvordering bevatten diverse bevoegdheden op grond waarvan grote hoeveelheden persoonsgegevens (ongericht) kunnen worden verzameld in het kader van een concreet opsporingsonderzoek. Naast de bevoegdheden met betrekking tot communicatie via aanbieders van communicatiediensten, moet in het bijzonder worden gedacht aan diverse vormen van onderzoek van gegevens in digitale-gegevensdragers en geautomatiseerde werken (al dan niet heimelijk; al dan niet op afstand) en het overnemen van daarop opgeslagen persoonsgegevens. Daarnaast kunnen persoonsgegevens op geautomatiseerde wijze uit open bronnen worden overgenomen⁶⁰ en kunnen derden op bevel, maar ook op verzoek vrijwillig persoonsgegevens verstrekken ten behoeve van het onderzoek.⁶¹

Door de vergaande digitalisering van de samenleving is steeds meer (persoonlijke) informatie digitaal beschikbaar. Door de snelle ontwikkeling van de technologie, vormen opslagcapaciteit, analysemogelijkheden en het (op afstand) verkrijgen van toegang tot digitale (versleutelde) gegevens niet of nauwelijks meer een beperking voor het verzamelen van grote hoeveelheden data. Het is begrijpelijk dat de opsporing van de digitale beschikbaarheid van gegevens en nieuwe technologie gebruik wil maken en dat hiervoor nieuwe bevoegdheden in het leven worden geroepen. Maar die bevoegdheden dragen ook meer dan ooit het risico in zich dat bij het verzamelen van gegevens ook persoonsgegevens ‘meekomen’ van onverdachte personen die niets te maken hebben met het strafbare feit waar het opsporingsonderzoek zich op richt. Het is mede daarom zaak dat de verwerking van deze gegevens zorgvuldig en evenredig plaatsvindt en nauwkeurig wordt genormeerd.

⁵⁹ De EDPB heeft in op 26 april 2023 richtsnoeren vastgesteld over het gebruik van gezichtsherkenningstechnologie in het Artikel 4, rechtshandavingsdomein (Richtsnoeren 05/2022).

⁶⁰ Artikel 2.8.8 voorstel voor vaststellingswet I.

⁶¹ Zie afdeling 7.3.3 inzake bevoegdheden in verband met de verstrekking van gegevens ten behoeve van het onderzoek en artikel 2.7.54 inzake het verzoek tot vrijwillige verstrekking in voorstel voor vaststellingswet I.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

Waarborgen hiervoor dienen niet alleen ‘aan de voorkant’ te worden getroffen (zoals normering van de gevallen waarin de gegevens mogen worden verzameld en de autoriteit die bevoegd is daartoe te beslissen), maar ook ‘aan de achterkant’, dat wil zeggen normering van het onderzoek dat aan deze gegevensverzamelingen mag worden verricht, de doelen waarvoor de gegevens mogen worden gebruikt en het tijdig vernietigen van niet (meer) relevante persoonsgegevens.

Verwerking van persoonsgegevens die met strafvorderlijke bevoegdheden zijn verzameld wordt in beginsel beheerst door de Wpg. Aan de Wpg lag oorspronkelijk de gedachte ten grondslag een nieuw evenwicht te verwezenlijken tussen de bescherming van de privacy van de burger enerzijds en het belang van de rechtshandhaving anderzijds.⁶² Maar deze wet, die in de jaren 2005-2007 tot stand is gekomen, is inmiddels verouderd, houdt onvoldoende rekening met de sterk gedigitaliseerde samenleving en voldoet niet meer aan de eisen die het huidige Europese (gegevensbeschermings)recht daaraan stelt. Dat geldt helemaal voor de verwerking van persoonsgegevens met betrekking tot onverdachte personen die onderdeel vormen van grote gegevensverzamelingen die op grond van strafvorderlijke bevoegdheden kunnen worden vergaard. De Wpg bevat onvoldoende waarborgen om de rechten en vrijheden van deze personen te beschermen, ook omdat de (verwerkings)verantwoordelijkheid voor de (verdere) verwerking van politiegegevens bij de korpschef ligt en niet bij het bevoegd gezag. Daarom is nieuwe regelgeving nodig.

In opdracht van het WODC heeft de Radboud Universiteit onderzoek gedaan naar de normering van het verwerken van persoonsgegevens voor strafvorderlijke doelen.⁶³ In dat kader hebben de onderzoekers behartigenswaardige aanbevelingen aan de wetgever gedaan. De AP betreurt het ten zeerste dat deze aanbevelingen niet hebben geleid tot concrete voorstellen in het voorliggende concept. In plaats daarvan heeft de wetgever ervoor gekozen de bestaande regels min of meer over te nemen in het voorliggende concept (Titel 1.7) met dien verstande dat de reikwijdte van die bepalingen zodanig is aangepast dat het beschermingsniveau substantieel is gedaald. Kort gezegd: de gevallen waarin gegevens moeten worden vernietigd zodra blijkt dat ze voor het onderzoek niet relevant zijn, worden ingeperkt ten opzichte van het huidige wetboek (artikel 2.1.19) en de bepalingen voor doelafwijkend gebruik (artikel 2.1.20) worden aanzienlijk opgerekt, zonder dat de noodzaak hiertoe is aangetoond. De AP is van oordeel dat de regeling voor het bewaren, vernietigen en doelafwijkend gebruik van strafvorderlijke gegevens nadere doordenking vergt die bovendien gelijke tred dient te houden met de introductie van nieuwe bevoegdheden voor het ongericht verzamelen van persoonsgegevens.

5.4.1 Bewaren en vernietigen van persoonsgegevens (artikelen 2.1.18 en 2.1.19)

Bij de introductie van de eerste technologische opsporingsbevoegdheid – de telefoontap – in 1971 was de wetgever zich al bewust van het feit dat daarmee ongericht gegevens werden verzameld die ook personen konden betreffen die geen enkele betrokkenheid bij het op te sporen strafbare feit hebben. Daarom werd naast de introductie van deze bevoegdheid tevens bepaald dat de gegevens die niet voor het onderzoek van

⁶² Kamerstukken II 2005/06, 30 327, nr. 3, p. 1.

⁶³ M.I. Fedorova, R.M. te Molder, M.J. Dubelaar, S.M.A. Lestrade en T.F. Walree, *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Radboud University Press, 2022.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

betekenis waren zo spoedig mogelijk moesten worden vernietigd.⁶⁴ Als gevolg van de opkomst van computers, werd in 1993 de bevoegdheid geregeld om gegevens die tijdens een doorzoeking op een computer (netwerk) werden aangetroffen vast te leggen voor de opsporing. Ook voor deze bevoegdheid is geregeld dat de gegevens die daarmee worden verzameld en van geen betekenis zijn voor het onderzoek, moeten worden vernietigd.⁶⁵ Bij de introductie van de 'hackbevoegdheid' in 2019 is wederom aangesloten bij deze regeling: zodra blijkt dat de met de hackbevoegdheid verzamelde gegevens voor het onderzoek van geen betekenis zijn, moeten deze worden vernietigd.⁶⁶ Ten slotte is eenzelfde regeling in 2022 geïntroduceerd voor gegevens die op een inbeslaggenomen smartphone na het moment van inbeslagneming zijn ontvangen en vastgelegd.⁶⁷ Deze bepalingen zijn van groot belang om te voorkomen dat persoonsgegevens van onschuldige personen die geen betrokkenheid bij strafbare feiten hebben in de politiestructuren belanden zonder dat daarvoor een legitieme reden bestaat.⁶⁸

Deze vernietigingsplicht sluit aan bij twee belangrijke beginselen voor de verwerking van persoonsgegevens die ook in het rechtshandavingsdomein gelden: het beginsel van dataminimalisatie en het beginsel van opslagbeperking.⁶⁹ Overweging 26 van de RGR verwoordt dit als volgt: *“De persoonsgegevens moeten toereikend en ter zake dienend zijn voor de doeleinden waarvoor zij worden verwerkt. Meer bepaald moet ervoor worden gezorgd dat niet bovenmatig veel gegevens worden verzameld en dat zij niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor zij worden verwerkt.”*

Gelet op de hiervoor gesignaleerde technologische ontwikkelingen in samenhang met de uitbreiding van bevoegdheden tot het ongericht verzamelen van bulkgegevens, had uitbreiding van deze regeling voor de hand gelegen.⁷⁰ In plaats daarvan heeft de wetgever, om praktische redenen, ervoor gekozen om deze vernietigingsplicht te beperken tot gegevens die zijn verkregen met de hackbevoegdheid (artikel 2.1.19). Reden hiervoor zijn de uitvoeringsproblemen die de opsporing in de huidige praktijk al ervaart met de toepassing van de vernietigingsplicht uit artikel 125n, zo blijkt uit de toelichting. *“Die uitvoeringsproblemen houden verband met de druk op de capaciteit die de opsporing ervaart met de uitvoering van het huidige artikel 125n. Door de digitale ontwikkelingen [...] verkrijgt de politie thans door de uitoefening van de strafvorderlijke bevoegdheden veel meer gegevens dan vroeger. Het huidige artikel 125n wordt zo ervaren dat de opsporing uit die enorme hoeveelheden gegevens relatief snel moet selecteren welke gegevens zij wil behouden voor het onderzoek waarna de overige gegevens moeten worden vernietigd omdat die van geen betekenis zijn voor het onderzoek. Daartoe is het nodig om schaarse (digitale) opsporingscapaciteit te belasten met het vernietigen van gegevens die niet van belang zijn. Deze capaciteit is dan niet beschikbaar voor het verder brengen van de zaak.”* Deze motivering overtuigt de AP geenszins. De fundamentele rechten en vrijheden van onschuldige personen kunnen niet op deze manier worden afgewogen tegen uitvoeringsconsequenties van zo praktische aard. Er zijn met wat goede wil en mogelijk enige extra financiering immers ook technische en organisatorische oplossingen voor de vernietiging van gegevens denkbaar die niet ten koste hoeven te gaan van de capaciteit voor de opsporing. In het verlengde

⁶⁴ Artikel 125h oud Sv.

⁶⁵ Artikel 125n Sv.

⁶⁶ Artikel 126cc, zesde lid, Sv.

⁶⁷ Artikel 556, zevende lid, jo. artikel 125n Sv.

⁶⁸ Vgl. A.L. Melai/M.S. Groenhuijsen e.a., *Wetboek van Strafvordering*, artikel 125n, aant. 4 (actueel t/m 18 juli 2008).

⁶⁹ Artikel 4, eerste lid, onderdelen c en e, van de RGR.

⁷⁰ Zie ook A.L. Melai/M.S. Groenhuijsen e.a., *Wetboek van Strafvordering*, artikel 125n, aant. 5 (actueel t/m 18 juli 2008).



Datum
3 maart 2025

Ons kenmerk
z2024-014439

hiervan merkt de AP nog op dat het de opsporing zelf is die de genoemde 'enorme hoeveelheden gegevens' verzamelt. Een nauwkeuriger selectie aan de voorkant is daarom ook vanuit dit perspectief noodzakelijk.

In de toelichting wordt voorts aangegeven dat de regeling tot problemen leidt in verband met de zogeheten forensische kopie. Dit is een volledige kopie van de bestanden die met toepassing van bepaalde bevoegdheden zijn vastgelegd of overgenomen. Zodra onderzoek aan de verzamelde bestanden en gegevens heeft plaatsgevonden, zouden niet alleen de niet relevante gegevens moeten worden vernietigd, maar – zo stelt de conceptmemorie van toelichting – strikt genomen ook de forensische kopie. De AP is van oordeel dat de vernietigingsplicht van niet-relevante gegevens samen kan gaan met een nauwkeurige regeling voor het – met name in het belang van de verdediging – afgeschermd (in een digitale kluis) bewaren van een volledige forensische kopie gedurende het onderzoek en het verloop van de strafzaak. Nadat de zaak is geëindigd moet dan ook de forensische kopie worden vernietigd.

Het huidige wetboek kent naast de hiervoor besproken vernietigingsplicht voor niet-relevante gegevens nog een tweede regeling voor het bewaren en vernietigen van op ongeselecteerde wijze verzamelde (persoons)gegevens. Dit betreft de regeling van artikel 126cc, eerste t/m derde lid, Sv. Voor dergelijke gegevens geldt dat, voor zover zij (nog) niet in de processtukken zijn opgenomen en de strafzaak nog niet is geëindigd, deze gegevens door de officier van justitie worden bewaard en ter beschikking worden gehouden van het onderzoek. Is de strafzaak geëindigd of zal het onderzoek naar redelijke verwachting niet tot een zaak leiden, dan moeten de gegevens worden vernietigd. Aan deze regeling ligt dezelfde ratio ten grondslag als aan de hiervoor besproken regeling van artikel 125n, zij het dat in deze regeling de niet-relevante gegevens pas na beëindiging van de strafzaak worden vernietigd.⁷¹ Hierdoor blijven dergelijke gegevens langer beschikbaar, namelijk zolang de zaak niet is geëindigd.

In het voorliggende concept is deze regeling als uitgangspunt genomen en neergelegd in artikel 2.1.18. De AP is van oordeel dat deze regeling aanzienlijk minder waarborgen biedt voor personen die geen betrokkenheid hebben bij de strafbare feiten waar het onderzoek zich op richt. De niet-relevante gegevens worden immers aanzienlijk langer bewaard dan onder de regeling van artikel 2.1.19 is toegestaan. Daardoor neemt het risico op oneigenlijk of onbevoegd gebruik van de verzamelde gegevens toe.

In aanvulling op het voorgaande, constateert de AP dat de artikelen 2.1.18 en 2.1.19 niets regelen voor persoonsgegevens die zijn verkregen op basis opsporingsbevoegdheden die niet in deze artikelen expliciet worden genoemd, maar op grond waarvan wel gegevens kunnen worden verzameld die ook gegevens over onverdachte personen omvatten. Dit stuit om de volgende redenen op bezwaren.

Het gaat in de eerste plaats om persoonsgegevens die zijn overgenomen uit publiek toegankelijke bronnen.⁷² De officier van justitie kan op grond van het in het voorstel voor vaststellingswet I neergelegde artikel 2.8.8 bevelen dat een opsporingsambtenaar stelselmatig, al dan niet op geautomatiseerde wijze, persoonsgegevens overneemt uit publiek toegankelijke bronnen. Aangezien deze bevoegdheid niet is beperkt tot persoonsgegevens betreffende de verdachte en bovendien de bevoegdheid op

⁷¹ Kamerstukken II 1996/97, 25 403, nr. 3, p. 86.

⁷² Artikel 2.8.8, voorstel voor vaststellingswet I.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

geautomatiseerde wijze kan worden uitgeoefend (bijv. met behulp van een webcrawler), zal deze bevoegdheid hoogstwaarschijnlijk ook leiden tot het verzamelen van (grote hoeveelheden) persoonsgegevens van niet-verdachte personen. Van belang is dat de wetgever kennelijk niet voornemens is eisen te stellen aan de inhoud van het bevel van de officier van justitie om deze verzameling van persoonsgegevens in te kaderen. Immers, het bevel tot toepassing van deze bevoegdheid is uitgezonderd van de algemene verplichting om bevelen tot inzet van heimelijke bevoegdheden afzonderlijk op schrift te stellen.⁷³ Dit brengt me zich dat voor dergelijke bevelen geen eisen (bij algemene maatregel van bestuur) zullen worden gesteld aan de gegevens die een dergelijk bevel moet bevatten (zoals bijvoorbeeld een omschrijving van het soort gegevens dat mag worden overgenomen, van de persoon of personen ten aanzien van wie die gegevens mogen worden overgenomen of van de bronnen waaruit persoonsgegevens mogen worden overgenomen).⁷⁴ Gelet hierop moet ervan worden uitgegaan dat deze bevoegdheid kan leiden tot het ongericht verzamelen van grote hoeveelheden persoonsgegevens. De AP is daarom van oordeel dat op zijn minst ook voor de gegevensverzamelingen die met deze bevoegdheid tot stand komen, een specifieke regeling moet worden getroffen voor het vernietigen van persoonsgegevens met betrekking tot personen die geen enkele betrokkenheid hebben bij het op te sporen strafbare feit en voorts dat het doelafwijkend gebruik van deze gegevens moet worden ingeperkt en van meer waarborgen moet worden voorzien (zie hierna paragraaf 5.4.2).

Min of meer hetzelfde geldt voor historische en toekomstige persoonsgegevens die zijn verzameld op basis van een bevel tot verstrekking daarvan⁷⁵ of die op verzoek van een opsporingsambtenaar vrijwillig zijn verstrekt.⁷⁶ De AP is van oordeel dat de vernietigingsplicht ook van toepassing zou moeten zijn op persoonsgegevens die langs deze weg zijn verzameld en van geen betekenis voor het onderzoek blijken te zijn. Ook deze bevoegdheden kunnen immers leiden tot de verstrekking van grote gegevensbestanden waarin veelal ook personen zullen voorkomen die met het te onderzoeken strafbare feit niets van doen hebben.⁷⁷ Dit geldt temeer omdat naar huidig recht de vordering tot verstrekking van gegevens in ieder geval dient te bepalen (a) indien bekend, de naam of anderszins een zo nauwkeurig mogelijke aanduiding van de persoon of de personen over wie gegevens worden gevorderd en (b) een zo nauwkeurig mogelijk aanduiding van de gegevens die worden gevorderd.⁷⁸ In het nieuwe wetboek komen deze vereisten niet terug. Het is nog onduidelijk of deze eisen zullen worden opgenomen in de algemene maatregel van bestuur die op grond van artikel 2.1.15 van het voorstel voor vaststellingswet I moet worden opgesteld.

Ten slotte is de AP van oordeel dat de vernietigingsplicht van voor het onderzoek niet-relevante gegevens ook van toepassing moet zijn op persoonsgegevens die zijn verzameld in het kader van onderzoek naar misdrijven die in georganiseerde verband worden beraamd of gepleegd en in geval van aanwijzingen van

⁷³ Zie artikel 2.8.1, eerste lid, jo. artikel 2.8.8 voorstel voor vaststellingswet I.

⁷⁴ Zie artikel 2.1.15, tweede lid, jo. artikel 2.8.1, eerste lid, voorstel voor vaststellingswet I.

⁷⁵ Artikel 2.7.46 en 2.7.49, voorstel voor vaststellingswet I.

⁷⁶ Artikel 2.7.54, voorstel voor vaststellingswet I.

⁷⁷ Dit geldt temeer omdat een nieuwe bevoegdheid wordt geïntroduceerd voor het geven van een generiek bevel tot verstrekking van gegevens aan "een ieder van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot die gegevens" (artikel 2.7.46, zesde lid, voorstel vaststellingswet I).

⁷⁸ Artikel 126nd, derde lid, Sv.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

een terroristisch misdrijf (artikel 2.7.53 en 2.8.22). Vooralsnog blijkt dit niet uit de tekst van de wet en de toelichting.

5.4.2 Doelafwijkend gebruik van persoonsgegevens (artikel 2.1.20)

Net als de AVG, bevat ook de RGR het beginsel van doelbinding als algemeen geldend beginsel voor de verwerking van persoonsgegevens. Dit beginsel – dat ook als algemeen rechtsbeginsel in artikel 8, tweede lid, van het Handvest is verankerd - houdt in dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt.⁷⁹ De AVG bevat voorts een opsomming van factoren waarmee in ieder geval rekening moet worden gehouden bij de beoordeling of een verdere verwerking van voor een bepaald doel verzamelde persoonsgegevens als verenigbaar kan worden beschouwd met het oorspronkelijke doel.⁸⁰ De RGR kent een dergelijke opsomming niet, maar bevat wel de eis dat de verwerking van persoonsgegevens voor een ander doel dan het doel waarvoor zij zijn verzameld alleen is toegestaan indien – kort gezegd - dit noodzakelijk en proportioneel is en voorzien is bij wet.⁸¹

De eis dat doelafwijkend gebruik van verzamelde persoonsgegevens op een wettelijke grondslag moet zijn gebaseerd is in het stelsel van de RGR ook logisch omdat de verwerking van persoonsgegevens onder die richtlijn alleen dan rechtmatig is als deze noodzakelijk is voor de taakuitvoering van bevoegde autoriteiten en is gebaseerd op het Unie- of nationale recht.⁸²

Zoals ook de onderzoekers van de Radboud Universiteit constateren, biedt de RGR voor het overige beperkte duidelijkheid als het gaat om de invulling en reikwijdte van het doelbindingsbeginsel.⁸³ Uit de uitspraak van het Hof van Justitie van 8 december 2022 volgt dat het Hof in ieder geval van oordeel is dat de verwerking van persoonsgegevens in het kader van de *opsporing* van een strafbaar feit een ander doel betreft dan de verwerking van die gegevens in het kader van een daaropvolgende *vervolg*ing van het opgespoorde strafbare feit.⁸⁴ In deze zaak ging het om gegevens van een persoon die in eerste instantie als slachtoffer in het opsporingsonderzoek voorkwam, maar later als verdachte in diezelfde zaak werd vervolgd. Het Hof acht dit doelafwijkende gebruik toegestaan, mits is voldaan aan de vereisten van een wettelijke grondslag, noodzakelijkheid en proportionaliteit.

Uit overweging 27 van de RGR blijkt dat persoonsgegevens die zijn verzameld in het kader van de voorkoming, het onderzoek, de opsporing en de vervolging van bepaalde strafbare feiten, ook buiten dat kader moeten kunnen worden verwerkt, teneinde inzicht te verwerven in criminele activiteiten en verbanden te leggen tussen verschillende opgespoorde strafbare feiten. Ook hieruit kan worden afgeleid dat – mits aan de voorwaarden van artikel 4, tweede lid, van de RGR is voldaan – gebruik van onder de

⁷⁹ Artikel 5, eerste lid, onder b, AVG en artikel 4, eerste lid, onder b, RGR.

⁸⁰ Artikel 6, vierde lid, AVG.

⁸¹ Artikel 4, tweede lid, RGR.

⁸² Artikel 8 RGR.

⁸³ M.I. Fedorova e.a., *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Radboud University Press, 2022, p. 153. Zie o.a. ook R.M. te Molder e.a., *Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing*, Computerrecht 2023/64.

⁸⁴ HvJEU 8 december 2022, C-180/21 (*Inspektor v Inspektorata kam Visshia sadeben savet*).



Datum
3 maart 2025

Ons kenmerk
z2024-014439

richtlijn verzamelde persoonsgegevens voor een ander doel dan waarvoor zij zijn verzameld wel is toegestaan.

Gelet op de waarborgfunctie van het doelbindingsbeginsel, achten de onderzoekers van de Radboud Universiteit het verdedigbaar dat het beginsel zo moet worden uitgelegd, dat de met (heimelijke) opsporingsbevoegdheden verkregen gegevens in beginsel alleen mogen worden gebruikt voor het concrete doel waarvoor de bevoegdheid is ingezet. Uit het in het voorliggende concept voorgestelde artikel 2.1.20 kan worden afgeleid dat de wetgever eenzelfde standpunt inneemt: de persoonsgegevens die zijn verkregen bij de uitoefening van een van de in artikel 2.1.20 genoemde opsporingsbevoegdheden mogen in beginsel alleen worden verwerkt in het kader van het onderzoek waarbinnen die bevoegdheid is ingezet. Alleen voor zover artikel 2.1.20 dit toelaat, kunnen deze gegevens worden gebruikt voor een ander doel.

Van belang hierbij is het volgende. Zowel de Wet politiegegevens als het Wetboek van Strafvordering bevatten regels over het bewaren, vernietigen en doelafwijkende gebruik van met opsporingsbevoegdheden verzamelde persoonsgegevens. De Wpg bevat hiervoor een meer algemene regeling; de regeling in het Wetboek van Strafvordering vormt hierop een *lex specialis* en inperking van die algemene regeling in de Wpg.⁸⁵ Aangezien, zoals hiervoor al is aangegeven, de bepalingen uit de Wpg niet goed meer aansluiten bij de huidige gedigitaliseerde samenleving en de Europese rechtsontwikkeling, zijn specifieke bepalingen in het nieuwe Wetboek van Strafvordering noodzakelijk om de grondrechten van (niet-verdachte) burgers te waarborgen. Beseft moet worden dat de verzamelde persoonsgegevens die niet onder de reikwijdte van specifieke bepalingen in het Wetboek van Strafvordering vallen, onder het algemene en (te) ruime regime van de Wpg komen te vallen. Omdat het huidige regime van de Wpg onvoldoende waarborgen bevat ter bescherming van de rechten en vrijheden van personen die geen verdachte zijn in een onderzoek en ook geen enkele betrokkenheid hebben bij het plegen of beramen van strafbare feiten, is aanvullende regelgeving nodig. Die waarborgen moeten naar het oordeel van de AP ook omvatten een toetsing door een rechter (of een onafhankelijke bestuurlijke autoriteit) voorafgaand aan de beslissing om grote hoeveelheden persoonsgegevens voor een ander doel beschikbaar te stellen dan het opsporingsonderzoek in welk kader ze zijn verzameld.

Het voorgestelde artikel 2.1.20 heeft alleen betrekking op doelafwijkend gebruik van gegevens waarvoor op grond van artikel 2.1.18 en 2.1.19 een vernietigingsplicht bestaat, zoals hiervoor in paragraaf 5.4.1 beschreven. De bezwaren die de AP in paragraaf 5.4.1 heeft geuit ten aanzien van de beperkte reikwijdte van de vernietigingsplicht gelden *mutatis mutandis* voor de beperkte reikwijdte van artikel 2.1.20.

Naar huidige recht⁸⁶ is het doelafwijkend gebruik van gegevens die zijn verzameld met de inzet van bijzondere opsporingsbevoegdheden slechts toegestaan voor:

- (a) een ander strafrechtelijk onderzoek; of
- (b) verwerking met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij misdrijven en handelingen als bedoeld in artikel 10, eerste lid, onder a en b, van de Wpg (kort

⁸⁵ Zoals bijvoorbeeld artikel 9, derde lid, Wpg ten aanzien van het doelafwijkende gebruik.

⁸⁶ Artikel 125n, derde lid en artikel 126dd, eerste lid, Sv.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

gezegd: inzicht in betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde).

Dit doelafwijkende gebruik is alleen toegestaan indien de officier van justitie daartoe heeft beslist.

In de voorgestelde regeling (artikel 2.1.20, eerste lid) is het *uitgangspunt* dat de officier van justitie kan bevelen dat gegevens die met de inzet van de in dat artikel genoemde opsporingsbevoegdheden zijn verzameld, in afwijking van het oorspronkelijk doel kunnen worden gebruikt voor:

- (a) een ander opsporingsonderzoek; of
- (b) een ander doel op grond van de Wpg of de Wjsg.

Gaat het om gegevens die zijn verzameld bij de aanbieder van een communicatiedienst, dan geldt op grond van artikel 2.1.20, tweede lid, dat de officier van justitie kan bevelen dat deze gegevens kunnen worden gebruikt voor:

- (a) een ander opsporingsonderzoek voor zover dat opsporingsonderzoek is gericht op een verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van vier jaar of meer is gesteld; of
- (b) een ander doel op grond van de Wpg of de Wjsg voor zover dat andere doel betrekking heeft op de voorkoming van ernstige bedreigingen van de openbare veiligheid.

Gaat het om gegevens die zijn verkregen met toepassing van de 'hackbevoegdheid' dan kan de officier van justitie bevelen dat deze op grond van het derde lid van artikel 2.1.20 worden gebruikt voor:

- (a) een ander opsporingsonderzoek voor zover dat opsporingsonderzoek is gericht op een verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van vier jaar of meer is gesteld;
- (b) het verkrijgen van inzicht in de betrokkenheid van personen bij misdrijven en handelingen als bedoeld in artikel 10, eerste lid, onderdelen a en b, van de Wpg.

Aan de gekozen opzet van artikel 2.1.20 ligt - zo blijkt uit de toelichting - het evenredigheidsbeginsel ten grondslag. Onder verwijzing naar relevante jurisprudentie van het Hof van Justitie, is aangegeven dat het evenredigheidsbeginsel met zich meebrengt dat de verdere verwerking van gegevens moet zijn gerechtvaardigd door het doel van die verdere verwerking. Verwezen wordt naar rechtspraak van het Hof van Justitie waaruit blijkt dat de verwerking van gegevens waarmee de rechten en vrijheden van betrokkenen ernstig worden beperkt, slechts kan worden gerechtvaardigd door de bestrijding van ernstige criminaliteit. Is de inmenging in de betrokken grondrechten daarentegen niet ernstig, dan kan de verwerking worden gerechtvaardigd door de doelstelling van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten in het algemeen (dus zonder de beperking dat het om ernstige criminaliteit moet gaan).⁸⁷

De AP kan deze gedachtegang op zichzelf volgen, maar heeft bezwaar tegen de wijze waarop dit in het voorstel voor artikel 2.1.20 is uitgewerkt. In de eerste plaats omdat in het nieuwe artikel 2.1.20, eerste en tweede lid, de mogelijkheden voor doelafwijkend gebruik, zonder nadere onderbouwing, aanzienlijk

⁸⁷ HvJEU 2 oktober 2018 C-207/16 ECLI:EU:C:2018:788 (*Ministerio Fiscal*), punt 55-57.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

worden uitgebreid ten opzichte van het huidige wetboek, in het bijzonder door de formulering 'een ander doel op grond van de Wpg of Wjsg'. Dit is immers aanzienlijk ruimer dan de huidige verwijzing die is beperkt tot het doel van artikel 10, eerste lid, onder a en b, van de Wpg.⁸⁸ De voorgestelde formulering maakt het namelijk mogelijk om met ingrijpende opsporingsbevoegdheden (ongericht) verzamelde persoonsgegevens - waarvoor in beginsel een vernietigingsplicht geldt of zou moeten gelden - bijvoorbeeld ook te gebruiken voor de dagelijkse politietoek, zoals de handhaving van de openbare orde en de hulpverleningstaak.⁸⁹ Deze doelen staan in geen enkele verhouding tot de inbreuk die op de grondrechten van betrokkenen is gemaakt bij het initiële verzamelen van die persoonsgegevens en de inbreuk die wordt gemaakt bij het verdere gebruik van die gegevens. Dit maakt de regeling disproportioneel. Zoals gezegd, de noodzaak voor deze uitbreiding wordt niet onderbouwd, terwijl de bescherming van de persoonlijke levenssfeer en van persoonsgegevens van personen die onderdeel kunnen vormen van de hier bedoelde gegevensverzamelingen, maar geen betrokkenheid hebben bij strafbare feiten door deze verruiming substantieel afneemt.

In het tweede lid van artikel 2.1.20 is een strengere regeling voor doelafwijkend gebruik opgenomen. Deze wordt toegelicht onder verwijzing naar de rechtspraak van het Hof van Justitie met betrekking tot de eis dat toegang tot verkeers- en locatiegegevens bij aanbieder van communicatiediensten slechts is toegestaan voor de bestrijding van ernstige criminaliteit (zie ook paragraaf 5.3.1 van deze wetgevingstoets). De voorgestelde strengere regeling (met dus beperktere mogelijkheden voor doelafwijkend gebruik) heeft uitsluitend betrekking op gegevens die zijn verzameld bij aanbieders van communicatiediensten. De AP is echter ook (en misschien wel juist) bezorgd over het doelafwijkend gebruik van grote hoeveelheden (persoons)gegevens die (ongericht) zijn verzameld met andere opsporingsbevoegdheden. Te denken valt hierbij aan de gegevens die zijn overgenomen uit een digitale-gegevensdrager, een geautomatiseerd werk of uit publiek toegankelijke bronnen of gegevens die op bevel of verzoek van een opsporingsambtenaar zijn verstrekt. De verdere verwerking van dergelijke gegevens voor een ander doel dan het opsporingsonderzoek waarin de gegevens zijn verzameld kan een grote impact hebben op personen die daarin voorkomen maar geen betrokkenheid hebben bij het strafbare feit waar het initiële onderzoek zich op richtte. Zo kan het overnemen van persoonsgegevens uit publiek toegankelijke bronnen voor de verdachte in een concreet onderzoek in welk kader de gegevens zijn verzameld mogelijk als geringe inbreuk op zijn grondrechten worden gezien. Maar wanneer die gegevensverzameling verder wordt verwerkt ten aanzien van personen die met het initiële opsporingsonderzoek niets van doen hebben, maar die wel onderdeel zijn van de verzamelde gegevens, dan kan die verdere verwerking ten aanzien van die andere personen wel als ernstige inmenging in het recht op bescherming van persoonsgegevens worden aangemerkt. Zie ook de in paragraaf 5.3 aangehaalde rechtspraak van het Hof van Justitie waaruit volgt dat het Hof ook bijzondere aandacht schenkt aan het feit dat persoonsgegevens op ongedifferentieerde of ongerichte wijze zijn verzameld alsmede het risico dat daarbij ook bijzondere persoonsgegevens worden verzameld. Bovenstaande noties komen in de regeling voor het doelafwijkend gebruik van verzamelde persoonsgegevens nog onvoldoende tot uitdrukking.

⁸⁸ In de toelichting wordt gesteld dat artikel 2.1.20, eerste lid, overeenkomt met het huidige recht. Zonder nadere uitleg kan deze stelling echter niet worden gevolgd.

⁸⁹ Zie artikel 8 Wpg jo. artikel 3 Politiewet.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

Daarbij merkt de AP nog op dat de voorgestelde algemene formulering ('een doel onder de Wpg of Wjsg') naar haar oordeel niet voldoet aan de eis die uit de rechtspraak van het Hof van Justitie en het Europees Hof voor de Rechten van de Mens voortvloeit dat wettelijke bepalingen die inmenging in het recht op bescherming van persoonsgegevens legitimeren voldoende duidelijk en nauwkeurig moeten zijn zodat de toepassing ervan voorspelbaar is voor degenen op wie deze bepalingen van toepassing zijn.⁹⁰

Gelet op het voorgaande is de AP van oordeel dat de voorgestelde regeling voor doelafwijkend gebruik in artikel 2.1.20 nadere doordenking en aanscherping behoeft waarbij meer rekening wordt gehouden met de impact van de verdere verwerking op andere personen dan de verdachte tegen wie het onderzoek in welk kader de gegevens zijn verzameld zich richtte. Aanpassing is naar het oordeel van de AP noodzakelijk om onverenigbaarheid met het Unierecht te voorkomen.

De AP voelt zich ook nog genoodzaakt een opmerking te maken over het doelafwijkend gebruik van persoonsgegevens die zijn verzameld in het kader een verkennend onderzoek. In het nieuwe wetboek wordt ook de bevoegdheid tot een verkennend onderzoek opgenomen.⁹¹ Dit is een onderzoek dat zich kan richten op bepaalde sectoren van de samenleving om vast te stellen of en op welke wijze in die sectoren criminaliteit voorkomt, zonder dat sprake is van een concrete verdenking van een strafbaar feit, maar waarbij noodzakelijkerwijs gegevens worden betrokken van onverdachte personen om uiteindelijk tot een verdenking te kunnen komen, aldus de memorie van toelichting bij het voorstel voor vaststellingswet I.⁹² In het nieuwe wetboek wordt voorgesteld de bevoegdheid tot het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen ook mogelijk te maken in het kader van een verkennend onderzoek.⁹³ In de memorie van toelichting is aangegeven dat de verwerking van persoonsgegevens in het kader van een verkennend onderzoek onder de Wpg valt en dat het niet wenselijk is dat deze gegevens (over onverdachte personen) tijdens het verkennend onderzoek ter beschikking worden gesteld met het oog op de verwerking voor andere doelen binnen de politietaak. Om dit te voorkomen, wordt in de memorie van toelichting bij de vaststellingswet I voorgesteld het Besluit politiegegevens in die zin aan te passen dat daarin een weigeringsgrond zal worden opgenomen om gegevens uit een verkennend onderzoek voor andere doelen binnen de politietaak beschikbaar te stellen.⁹⁴ De AP acht deze regeling ontoereikend. De voorgestelde regeling⁹⁵ zou namelijk slechts de *mogelijkheid* bieden om de verstrekking van deze gegevens voor andere doelen binnen de politie te weigeren, maar niet de *verplichting*. De AP is dan ook van oordeel dat met deze voorgestelde regeling niet kan worden volstaan. Er dient een duidelijker bepaling, bij voorkeur op het niveau van de wet in formele zin, te worden opgesteld.

Ten slotte onderstreept de AP nog voor de goede orde dat het doelbindingsbeginsel (zie ook artikel 2.1.2, eerste lid, voorstel vaststellingswet I) uiteraard in den brede geldt voor gegevens die op basis van het Wetboek van Strafvordering zijn verkregen. Zo mogen bijvoorbeeld haren die op grond van artikel 2.6.16

⁹⁰ Zie ook overweging 33 RGR.

⁹¹ Artikel 2.9.1 voorstel vaststellingswet I. (huidige artikel 126gg Sv).

⁹² Kamerstukken II 2022/23, 36 327, nr. 3, p. 726.

⁹³ Artikel 2.9.1, tweede lid, voorstel vaststellingswet I.

⁹⁴ Kamerstukken II 2022/23, 36 327, nr. 3, p. 728.

⁹⁵ Aanpassing van artikel 2:13 Besluit politiegegevens.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

zijn afgeschoren van een verdachte met als doel een getuige met de verdachte te confronteren - zonder duidelijke en nauwkeurige wettelijke grondslag waaruit dit verdere gebruik voorzienbaar is - niet vervolgens worden gebruikt voor het buiten medeweten van de verdachte verrichten van DNA- of toxicologisch onderzoek. Hetzelfde geldt bijvoorbeeld voor vingerafdrukken die zijn afgenomen om de identiteit van de verdachte te verifiëren. Deze mogen niet worden gebruikt om vervolgens buiten medeweten van de verdachte bijv. een smartphone te ontgrendelen, tenzij hiervoor een duidelijke en nauwkeurige wettelijke grondslag wordt gecreëerd.

5.4.3 Verwerking van bijzondere persoonsgegevens

Een aantal bevoegdheden uit het Wetboek van Strafvordering leidt per definitie tot de verwerking van bijzondere persoonsgegevens in de zin van de RGR. Het gaat hierbij in het bijzonder om de bevoegdheden met betrekking tot het lichaam.⁹⁶ Vingerafdrukken en gezichtsopnamen bedoeld voor geautomatiseerde gezichtsvergelijking/-herkenning zijn biometrische persoonsgegevens. DNA-profielen zijn genetische persoonsgegevens. De resultaten van adem-, speeksel-, bloed- of urineonderzoek of van onderzoek aan ander lichaamsmateriaal, gericht op het vaststellen van alcohol- of drugsgebruik of van een ernstige besmettelijke ziekte leveren persoonsgegevens betreffende de gezondheid van de betrokkene op.

Bij deze bevoegdheden is niet alleen sprake van inmenging in het recht op lichamelijke integriteit en het recht op eerbiediging van het privéleven, maar ook van het recht op bescherming van persoonsgegevens. Zoals in paragraaf 5.3.3 van deze wetgevingstoets al is opgemerkt, stelt artikel 10 van de RGR strenge eisen aan de verwerking van dergelijke bijzondere persoonsgegevens. De verwerking daarvan moet strikt noodzakelijk zijn en is alleen toegestaan als hiervoor een duidelijke en nauwkeurige wettelijke grondslag bestaat.

Nu de Minister van Justitie en Veiligheid afziet van het opstellen van de eerder aangekondigde gegevensbeschermingswet voor politie en justitie, worden via het voorliggende concept ook de bepalingen betreffende de (verdere) verwerking van deze persoonsgegevens teruggeplaatst in het Wetboek van Strafvordering. Hiertoe breidt het concept de in het voorstel voor vaststellingswet I opgenomen algemene delegatiebepaling (artikel 2.6.5) uit, zodat deze ook een grondslag biedt voor regels betreffende de (verdere) verwerking van deze bijzondere persoonsgegevens. Daarnaast voegt het concept aan de bepalingen die strekken tot het afnemen van gezichtsopnamen en vingerafdrukken (artikel 2.6.9) en tot het afnemen van celmateriaal om DNA-profielen te bepalen voor klassiek DNA-onderzoek (artikel 2.6.17) en DNA-verwantschapsonderzoek (artikel 2.6.18) een lid toe waaruit volgt dat de afgenomen gezichtsopnamen, vingerafdrukken en DNA-profielen (kunnen) worden verwerkt “voor het voorkomen, opsporen, vervolgen en berechten van strafbare feiten en het vaststellen van de identiteit van een overleden persoon”. Deze tamelijk cryptische en onnauwkeurige omschrijving (overgenomen uit het huidige Wetboek van Strafvordering) is in de praktijk de grondslag gaan vormen voor het opnemen en bewaren van deze bijzondere persoonsgegevens in databanken met het doel deze persoonsgegevens verder te verwerken voor de opsporing en vervolging van toekomstige strafbare feiten. De AP onderstreept voor de goede orde nogmaals dat opneming in een databank kwalificeert als doelafwijkend gebruik, aangezien

⁹⁶ Boek 2, Hoofdstuk 6 van het voorstel voor vaststellingwet I.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

de persoonsgegevens daarin worden opgenomen voor een ander doel dan het opsporingsonderzoek in welk kader de persoonsgegevens zijn verzameld. Zoals in de vorige paragraaf is aangegeven, is dit doelafwijkend gebruik uitsluitend toegestaan als dit noodzakelijk en proportioneel is en is gebaseerd op een duidelijke en nauwkeurige wettelijke grondslag.

Het 1-op-1 vergelijken van een vingerspoot of DNA-spoor dat op een plaats delict is aangetroffen met een van vingerafdruk of een DNA-profiel van een (aangehouden) verdachte vormt alleen een inmenging in het recht op bescherming van persoonsgegevens van die verdachte. Wanneer het aangetroffen spoor echter geautomatiseerd wordt vergeleken met alle DNA-profielen of alle vingerafdrukken die in een databank zijn opgeslagen (1-op-veel) betreft dit een inmenging in het recht op bescherming van persoonsgegevens van alle personen die in de databank staan geregistreerd. Ditzelfde geldt voor het geautomatiseerd vergelijken van een beeldopname die van een vermoedelijke dader is gemaakt met in een databank vastgelegde gezichtsopnamen van personen. Het opnemen en bewaren van bijzondere persoonsgegevens in een databank voor opsporingsdoeleinden en het raadplegen van die databank vormen dus een aanzienlijke inbreuk op het recht op bescherming van persoonsgegevens die niet alleen een duidelijke en nauwkeurige grondslag behoeft, maar ook democratische legitimering door het parlement.

Gelet op de bijzondere bescherming die de Uniewetgever heeft beoogd te bieden voor de verwerking van dergelijke bijzondere persoonsgegevens (artikel 10 van de RGR), is de AP van oordeel dat de hoofdlijnen van de normering van deze gegevensverwerkingen op het niveau van een wet in formele zin moeten worden vastgesteld. Dit betekent dat in ieder geval de grondslag voor verdere verwerking (opslag) van dergelijke bijzondere persoonsgegevens in een databank ten behoeve van de opsporing van toekomstige misdrijven op het niveau van de wet moet zijn geregeld, met inachtneming van de eis dat opslag in een databank alleen is toegestaan wanneer dit in het concrete geval strikt noodzakelijk is.⁹⁷ Daarnaast moeten ook de voorwaarden waaronder een dergelijke databank kan worden geraadpleegd (voor welk soort strafbare feiten en wie moet toestemming geven) op het niveau van de wet in formele zin worden vastgelegd. De AP geeft in overweging te bezien of het wenselijk is te komen tot een 'kaderwet strafvorderlijke databanken' waaruit voor elke strafvorderlijke databank de belangrijke aspecten die verband houden met de inrichting en gebruik van die databank (zoals doel, soort gegevens, toegang, bewaartermijnen e.d.) kenbaar is.

Daarnaast wijst de AP nog op het volgende. Het huidige wetboek biedt in het geval van zwaarwegende redenen de mogelijkheid om ten behoeve van het klassieke DNA-onderzoek het daarvoor benodigde celmateriaal niet rechtstreeks van de verdachte af te nemen maar op andere wijze te verkrijgen, mits voldoende zekerheid bestaat dat het celmateriaal van de verdachte afkomstig is.⁹⁸ In de voorstellen voor het nieuwe wetboek worden de mogelijkheden voor deze alternatieve wijze van het verkrijgen lichaamsmateriaal aanzienlijk uitgebreid, zoals blijkt uit de volgende voorbeelden. Ook celmateriaal ten

⁹⁷ Zie ook HvJEU 30 januari 2024, C-118/22 ECLI:EU:C:2024:97 (NG), punt 42 ("Die opslag vormt overigens een inmenging in de grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens, ongeacht of de opgeslagen gegevens gevoelig zijn, of de betrokkenen door die inmenging enig nadeel hebben ondervonden, en of de opgeslagen gegevens daarna worden gebruikt.")

⁹⁸ Artikel 151b, vierde lid, en artikel 195d, vierde lid, Sv.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

behoefte van het DNA-verwantschapsonderzoek⁹⁹ en celmateriaal ten behoeve van het vaststellen van een ernstige besmettelijke ziekte¹⁰⁰ kan in geval van zwaarwegende redenen op een andere wijze dan rechtstreeks bij de verdachte worden verkregen. Datzelfde geldt voor lichaamsafdrukken,¹⁰¹ zoals handpalmafdrukken, gezichtsopnamen en vingerafdrukken.¹⁰² De AP wijst op de aanzienlijke risico's die hierbij bestaan wanneer de op alternatieve wijze verkregen gegevens worden toegeschreven aan een persoon/verdachte die een ander blijkt te zijn dan werd aangenomen. Er is immers geen zekerheid dat de onderzochte gegevens daadwerkelijk van de verdachte afkomstig zijn. Volgens de wet volstaat het wanneer slechts 'voldoende zekerheid' bestaat dat dit van de verdachte afkomstig is. Zeker wanneer deze gegevens vervolgens in een databank worden opgenomen, kan de onjuistheid hiervan zeer grote gevolgen voor de betrokkene hebben. De AP wijst in dit verband op artikel 4, eerste lid, onderdeel c, van de RGR waaruit volgt dat de verwerkte persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. Overweging 30 van de richtlijn voegt hier nog aan toe dat het beginsel van juistheid van gegevens moet worden toegepast met inachtneming van de *aard* en het *doel* van de verwerking in kwestie. Tegen deze achtergrond, dient uit de wet en toelichting te blijken welke maatregelen worden getroffen om de juistheid van de verwerking van deze gevoelige persoonsgegevens te waarborgen.

5.4.4 Verwerking van ANPR-kentekengegevens (artikel 6.5.13)

Het huidige artikel 126jj Sv, eerste lid, Sv voorziet in de bevoegdheid om op algemene en ongedifferentieerde wijze op de openbare weg door middel van ANPR-camera's kentekengegevens van alle passerende voertuigen vast te leggen met als doel deze te kunnen raadplegen voor (a) de opsporing van misdrijven waarop een gevangenisstraf van vier jaar of meer is gesteld of (b) de aanhouding van een voortvluchtige persoon met het oog op de tenuitvoerlegging van een aan hem opgelegde straf of maatregel. Op grond van artikel 126jj, derde lid, Sv kan de officier van justitie bevelen dat een opsporingsambtenaar de vastgelegde kentekens voor de eerder genoemde doelen raadpleegt. Deze bevoegdheid wordt in het nieuwe wetboek overgenomen in artikel 6.5.13 voorstel voor vaststellingswet I.

Omdat, zoals hiervoor al is vermeld, ervan wordt afgezien een afzonderlijke gegevensverwerkingswet voor het rechtshandavingsdomein op te stellen, worden de bepalingen ten aanzien van de verwerking van deze kentekengegevens door middel van het voorliggende concept teruggeplaatst in het nieuwe wetboek. Onder kentekengegevens worden in dit verband verstaan: het kenteken, een foto van het passerende voertuig alsmede de locatie en het tijdstip van het passeren van het voertuig.¹⁰³

⁹⁹ Zie in het concept voorgestelde wijziging van artikel 2.6.18, zesde lid, jo. artikel 2.6.17, vijfde lid.

¹⁰⁰ Zie in het concept voorgestelde wijziging van artikel 2.6.20, vierde lid.

¹⁰¹ Artikel 2.6.13, derde lid, voorstel voor vaststellingswet I.

¹⁰² Artikel 2.6.9, vijfde lid, voorstel voor vaststellingswet I.

¹⁰³ Artikel 6.5.13, tweede lid, voorstel vaststellingswet I.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

Uit de locatielijst ANPR-cameraplan 126jj WvSv eerste kwartaal 2025 blijkt dat de politie op ongeveer 973 locaties in Nederland de genoemde kentekengegevens op basis van artikel 126jj Sv vastlegt.¹⁰⁴ Op grond van de geldende regelgeving worden deze gegevens vier weken in een database bewaard.¹⁰⁵

In paragraaf 5.3.1 is ingegaan op de rechtspraak van het Hof van Justitie met betrekking tot op algemene en ongedifferentieerde wijze verzamelde en vastgelegde verkeers- en locatiegegevens respectievelijk passagiersgegevens. Het Hof van Justitie heeft bepaald dat voor de toegang tot deze persoonsgegevens voorafgaande toestemming door een rechter of onafhankelijk bestuursorgaan is vereist. Gelet op deze rechtspraak is de AP van oordeel dat ook voor de raadpleging van de op basis van artikel 6.5.13 vastgelegde persoonsgegevens een voorafgaande machtiging van de rechter-commissaris of een onafhankelijke bestuurlijke autoriteit zou moeten worden geïntroduceerd. De op grond van deze bevoegdheid verzamelde gegevens – die hoofdzakelijk betrekking hebben op onverdachte personen – kunnen immers in samenhang gezien inzicht verschaffen over bepaalde delen van het privéleven van de betrokkene, zoals bijvoorbeeld reisroutes, reisgewoontes, woon- en werklocaties.

Het concept stelt voor om het huidige artikel 125jj, vijfde lid, ongewijzigd over te nemen in het nieuwe Wetboek van Strafvordering.¹⁰⁶ Deze bepaling strekt ertoe te bepalen dat bepaalde onderdelen van de Wet politiegegevens niet van toepassing zijn op de vastgelegde en bewaarde kentekengegevens. Dit houdt bijvoorbeeld verband met het feit dat de gegevens (in tegenstelling tot de bewaartermijnen in de Wpg) na een maand moeten worden vernietigd en dat zij uitsluitend voor de in het Wetboek van Strafvordering genoemde doelen mogen worden geraadpleegd en gebruikt. Daarom is bepaald dat de artikelen paragraaf 2 Wpg inzake de verwerking van politiegegevens met het oog op de uitvoering van de politietaak, paragraaf 3 Wpg inzake de doorgifte of verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee en in paragraaf 5a Wpg inzake de verwerking van politiegegevens op Bonaire, Sint Eustatius en Saba niet van toepassing zijn. De artikelen 8, eerste lid, 17 en 17a van de Wpg zijn echter weer wél van toepassing op de vastgelegde en bewaarde kentekengegevens.

Dit stelsel en in het bijzonder de toepasselijkheid van artikel 8, eerste lid, Wpg stuit op bezwaren van de AP. Artikel 8, eerste lid, Wpg bepaalt dat politiegegevens kunnen worden verwerkt voor de dagelijkse politietaak. Hieronder valt niet alleen de opsporing van eenvoudige strafbare feiten, maar ook de handhaving van de openbare orde en de hulpverleningstaak. Uit het feit dat artikel 8, eerste lid, van de Wpg van toepassing is op de kentekengegevens die met de ANPR-camera's op grond van de hier besproken bevoegdheid worden vastgelegd en bewaard, zou kunnen worden afgeleid dat deze gegevens ook beschikbaar zijn voor de dagelijkse politietaak. Dit zou in strijd zijn met het Unierecht. Uit de in paragraaf 5.3.1 en 5.4.2 aangehaalde rechtspraak van het Hof van Justitie volgt namelijk dat wanneer persoonsgegevens worden verzameld en bewaard voor de opsporing van ernstige criminaliteit (i.c. de opsporing van misdrijven waarop een gevangenisstraf van vier jaar of meer is gesteld), de vastgelegde

¹⁰⁴ Stcrt. 2024, 42051. Zie voorts <https://www.politie.nl/informatie/locaties-cameraplan-anpr-126jj-sv.html>.

¹⁰⁵ Artikel 9, vierde lid, Besluit vaststelling nadere regels vastleggen en bewaren kentekengegevens ex artikel 126jj Wetboek van Strafvordering door politie.

¹⁰⁶ Vijfde lid van artikel 6.5.13, zoals voorgesteld in het concept.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

gegevens alleen voor dat doel of een hoger gelegen doel kunnen worden gebruikt.¹⁰⁷ Zoals hiervoor al is omschreven, worden de kentekengegevens vastgelegd en bewaard met als doel de opsporing van misdrijven waarop gevangenisstraf van vier jaar of meer is gesteld of aanhouding van een voortvluchtige persoon. Handhaving van de openbare orde, opsporing van eenvoudige delicten en het verlenen van hulp vallen niet binnen dit doel, waardoor de verdere verwerking voor deze ‘minder zware’ doelen naar het oordeel van de AP niet voldoet aan het evenredigheidsbeginsel en in strijd is met het Europese recht zoals door het Hof van Justitie uitgelegd.

Hoewel uit de wetsgeschiedenis met betrekking tot het huidige artikel 126jj Sv niet kan worden afgeleid dat de wetgever het gebruik van de gegevens voor de dagelijkse politietoekende taak destijds ook heeft beoogd,¹⁰⁸ dient de tekst van de wet klip en klaar te zijn dat deze gegevens uitsluitend voor de in het Wetboek van Strafvordering genoemde doelen mogen worden gebruikt. Verwijzing naar artikel 8, eerste lid, Wpg dient dan ook geschrapt te worden. Alleen wanneer de officier van justitie (na machtiging van de rechter-commissaris, zie hierboven) de raadpleging van deze gegevens heeft bevolen en die raadpleging tot een hit heeft geleid, mogen de desbetreffende gegevens in de gebruikelijke politiesystemen verder worden verwerkt.

Tenslotte stuit ook de ongeclausuleerde doorgifte aan derde landen (toepasselijkheid van artikel 17a Wpg) van de bewaarde kentekengegevens op bezwaren van de AP. Weliswaar is het denkbaar dat een derde land Nederland verzoekt om raadpleging van de kentekengegevens die op grond van de hier besproken bevoegdheid zijn vastgelegd en bewaard, maar duidelijk moet zijn dat een dergelijke verstrekking alleen dan is toegestaan indien deze geschiedt met het oog op de opsporing van ernstige criminaliteit of een voortvluchtige persoon en de officier van justitie bevel heeft gegeven voor het raadplegen van de vastgelegde gegevens. Deze randvoorwaarden blijken nu noch uit de tekst van de wet, noch uit de toelichting.

5.4.5 Onderzoek en geautomatiseerde data-analyse van persoonsgegevens

De Wetenschappelijke Raad voor het Regeringsbeleid (hierna: WRR) heeft in 2016 al geconstateerd dat er een hiaat bestaat bij de regulering van de fase van analyse van gegevens in het veiligheidsdomein en dat aanvullende normering noodzakelijk is.¹⁰⁹ Ook in het eerder genoemde onderzoek van de Radboud Universiteit en door anderen in de wetenschap,¹¹⁰ waaronder ook de projectgroep van wetenschappers die

¹⁰⁷ Zie HvJEU 2 oktober 2018 C-207/16 ECLI:EU:C:2018:788 (*Ministerio Fisca*).

¹⁰⁸ Uit de kamerstukken blijkt dat de wetgever strikte doelbinding heeft beoogd voor de op grond van artikel 126jj Sv vastgelegde kentekengegevens, zie bijv. Kamerstukken II 2015/16, 33 542, nr. 20, p. 5.

¹⁰⁹ Wetenschappelijke Raad voor het Regeringsbeleid, *Big data in een vrije en veilige samenleving*, Amsterdam University Press, 2016.

¹¹⁰ R.M. te Molder, M.J. Dubelaar, M.I. Fedorova, S.M.A. Lestrade en T.F. Walree, *Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing*, *Computerrecht* 2023/64; M.F.H. Hirsch Ballin, *Geautomatiseerde data-analyse in het nieuwe Wetboek van Strafvordering*, *Strafblad* 2024, nr. 1; B.W. Schermer en M. Galič, *Biedt de Wet politiegegevens een stelsel van ‘end-to-end’ privacywaarborgen?*, *Nederlands Tijdschrift voor Strafrecht* 2022/3; F.H. Hirsch Ballin en J.J. Oerlemans, *Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden*, *Delikt en Delinkwent* 2023/2; B. Schermer, *Het gebruik van Big Data voor opsporingsdoelstellingen: tussen Strafvordering en Wet politiegegevens*, *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2017, nr. 4.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

de Tweede Kamer bijstand verleent bij de behandeling van de voorstellen voor het nieuwe wetboek,¹¹¹ is geconstateerd dat onderzoek en data-analyse van grote gegevensverzamelingen waaruit o.a. nieuwe verdenkingen met nieuwe verdachten kunnen ontstaan, op dit moment onvoldoende is gereguleerd. De AP onderschrijft dit oordeel.

De wetgever geeft tot nu toe ook geen blijk van enige intentie om dit nader te reguleren. Integendeel, in het voorstel voor vaststellingswet I wordt namelijk voorgesteld om het bevel tot het verrichten van stelselmatig onderzoek van gegevens in een digitale-gegevensdrager of geautomatiseerd werk of gegevens die daaruit zijn overgenomen, uit te zonderen van de verplichting tot het afzonderlijk vastleggen van een bevel tot inzet van bevoegdheden met betrekking tot voorwerpen en gegevens.¹¹² Datzelfde geldt voor het bevel tot het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen. Ook dit bevel is uitgezonderd van de verplichting om bevelen tot inzet van heimelijke bevoegdheden afzonderlijk op schrift te stellen.¹¹³ Dit betekent dat dergelijke bevelen mondeling kunnen worden gegeven en dat er geen voorschriften gelden voor de elementen die zo'n bevel in ieder geval dient te bevatten. De AP acht dergelijke uitzonderingen onwenselijk omdat dit betekent dat het bevel tot het verrichten van dergelijke handelingen (min of meer) vormvrij is, terwijl nu juist bij deze bevoegdheden van belang is dat de officier van justitie of rechter-commissaris kaders geeft waarbinnen opsporingsambtenaren die bevoegdheden mogen toepassen. Zonder dergelijke kaders bestaat het risico op misbruik en onevenredige verwerking van persoonsgegevens. Bovendien kan deze vormvrije uitoefening van opsporingsbevoegdheden spanning opleveren met het grondrecht op een doeltreffende voorziening in rechte wanneer sprake is van een inbreuk op grondrechten.¹¹⁴

De vele strafzaken die zijn voortgekomen uit onderzoek en analyse van zeer grote gegevensbestanden die met het onderscheppen van versleutelde communicatie zijn verkregen (EncroChat, SkyECC, Ennetcom) tonen aan dat dit onderzoek waardevol kan zijn voor de opsporing van strafbare feiten, maar tegelijkertijd dat dat onderzoek en die analyse diverse rechtsvragen oproepen in verband met de rechtmatigheid daarvan en bovendien aanzienlijke gevolgen kan hebben voor personen die aanvankelijk geen voorwerp waren van het onderzoek in welk kader de gegevens zijn verzameld. Dergelijke gevolgen kunnen zich niet alleen voordoen bij onderzoek en analyse van in een specifiek opsporingsonderzoek verzamelde data, maar ook als gegevens die met verschillende doelen zijn verzameld en in verschillende systemen bij de politie beschikbaar zijn in samenhang worden onderzocht en geanalyseerd.

Tegen deze achtergrond onderschrijft de AP dan ook de aanbevelingen van de onderzoekers van de Radboud Universiteit om tot nadere normering van dergelijke vormen van onderzoek en data-analyse te komen van harte. Naar het oordeel van de AP kan deze normering niet los worden gezien van de normering van de bevoegdheden om grote hoeveelheden digitale (persoons)gegevens te verzamelen. Het Europees Hof voor de Rechten van de Mens heeft in 2021 twee belangrijke uitspraken gewezen waaruit

¹¹¹ Project bijstand Tweede Kamer modernisering wetboek van Strafvordering, Inhoudelijks rapportage Boek 2: Het opsporingsonderzoek, Vrije Universiteit, 11 september 2023. Radboud Universiteit, Universiteit Utrecht en Erasmus University Rotterdam, para. 7.4.7 en 8.4.3.

¹¹² Artikel 2.7.1, onder b, jo. artikel 2.7.38, voorstel voor vaststellingswet I.

¹¹³ Artikel 2.8.1, eerste lid, jo. artikel 2.8.8, voorstel voor vaststellingswet I.

¹¹⁴ Artikel 47 Handvest en artikel 54 RGR.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

blijkt dat het EHRM bij de beoordeling van de rechtmatigheid van het ongericht in bulk verzamelen van (persoons)gegevens niet slechts kijkt naar de mate waarin burgers worden geraakt door het in bulk verzamelen van die gegevens, maar dit mede beoordeelt aan de hand van het proces van onderzoek dat op de verzameling van de gegevens volgt.¹¹⁵ Het EHRM geeft aan dat de inbreuk op de persoonlijke levenssfeer toeneemt naar mate het onderzoek aan in bulk verzamelde gegevens vordert en zich meer toespitst op bepaalde personen. Verschillende fasen in dit onderzoek worden geïdentificeerd en het EHRM bepaalt dat in iedere fase de noodzaak en proportionaliteit moet worden beoordeeld. Deze meer 'holistische' benadering van het EHRM dwingt naar het oordeel van de AP ook tot een 'holistische' aanpak bij de modernisering van het Wetboek van Strafvordering. Daarbij zou ook moeten worden voorzien in een toetsende rol voor de rechter-commissaris. Van een dergelijke 'holistische' aanpak in het kader van het nieuwe Wetboek van Strafvordering is op dit moment nog geen sprake. Dit raakt ook aan het hierna volgende punt.

Zoals de WRR reeds in zijn eerder aangehaalde rapport uit 2016 opmerkte, zal bij de normering van onderzoek en data-analyse in het veiligheidsdomein ook bijzondere aandacht moeten uitgaan naar waarborgen in verband met de kwaliteit van de data die bij analyses wordt gebruikt (zie ook het in paragraaf 5.4.3 aangehaalde beginsel van juistheid) en eisen die aan de systemen worden gesteld die kunnen worden ingezet voor onderzoek en data-analyse. Zeker waar de toenemende wens bestaat om geavanceerde, al dan niet op AI gebaseerde analysetools in te zetten, is het van belang niet alleen de risico's van de inzet daarvan vooraf goed in kaart te brengen, maar ook specifieke regels hiervoor vast te stellen. Gebrekkige datakwaliteit en slecht functionerende algoritmes kunnen – zeker in het domein van rechtshandhaving – desastreuze gevolgen hebben voor individuen.

5.4.6 Doeltreffende voorziening in rechte en notificatieplicht

De AP vraagt ook bijzondere aandacht voor de implementatie van artikel 54 van de RGR waarin het in artikel 47 van het Handvest opgenomen grondrecht op een doeltreffende voorziening in rechte nader is uitgewerkt voor de RGR. Artikel 54 RGR bepaalt dat iedere betrokkene het recht heeft een doeltreffende voorziening in rechte in te stellen, indien hij van mening is dat een inbreuk is gepleegd op zijn rechten uit hoofde van krachtens de RGR vastgestelde bepalingen als gevolg van een verwerking van zijn persoonsgegevens die niet aan die bepalingen voldoet.

Uit vaste rechtspraak van het Hof van Justitie volgt dat het door artikel 47 van het Handvest gewaarborgde recht op een doeltreffende voorziening in rechte in beginsel vereist dat de belanghebbende kennis kan nemen van de gronden waarop het jegens hem genomen besluit is gebaseerd, teneinde hem de mogelijkheid te bieden zijn rechten onder zo goed mogelijke omstandigheden te verdedigen en met volledige kennis van zaken te beslissen of hij er baat bij heeft om zich tot de bevoegde rechter te wenden, en teneinde deze laatste ten volle in staat te stellen om de wettigheid van dit besluit te toetsen.

Tegelijkertijd benadrukt het Hof dat dit recht geen absolute gelding heeft en dat overeenkomstig artikel 52 van het Handvest beperkingen aan kunnen worden gesteld, op voorwaarde dat deze beperkingen bij wet

¹¹⁵ EHRM 25 mei 2021 (*Big Brother Watch e.a. t. VK*) en EHRM 25 mei 2021 (*Centrum för Rättvisa t. Zweden*).



Datum
3 maart 2025

Ons kenmerk
z2024-014439

worden gesteld, de wezenlijke inhoud van de betrokken rechten en vrijheden eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en de vrijheden van anderen.¹¹⁶

In de artikelen 2.7.35 en 2.8.2 van het voorstel voor vaststellingswet I zijn notificatieverplichtingen opgenomen die echter een beperkte reikwijdte kennen. Daarnaast bevat de Wpg algemene bepalingen over het informeren van betrokkenen over de verwerking van persoonsgegevens.¹¹⁷ De AP is van oordeel dat een nadere analyse moet worden uitgevoerd teneinde te beoordelen of deze bepalingen én de wijze waarop daaraan in de praktijk uitvoering wordt gegeven voldoende recht doen aan het grondrecht op een doeltreffende voorziening in rechte en de uitleg die het Hof van Justitie daaraan geeft. De AP heeft hierbij in het bijzonder zorgen over de mogelijkheden tot uitoefening van dit recht door personen die niet als verdachte in een strafzaak voor de rechter worden gebracht, terwijl hun grondrecht op bescherming van persoonsgegevens (of andere grondrechten) mogelijk wel is geschonden. De AP verwijst naar al hetgeen hiervoor is opgemerkt ten aanzien van het (ongericht of in bulk) verzamelen en verder verwerken van persoonsgegevens waaronder van personen die geen betrokkenheid hebben bij het beramen of plegen van strafbare feiten.

5.4.7 Verhouding Wetboek van Strafvordering tot de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens

Door de onderzoekers van de Radboud Universiteit is ook aandacht gevraagd voor de systematiek van de normering. Normering van het met toepassing van opsporingsbevoegdheden *verzamelen* van persoonsgegevens met het oog op het onderzoek en de opsporing van strafbare feiten is van oudsher geregeld in het Wetboek van Strafvordering terwijl regels over het (verder) verwerken van dergelijke persoonsgegevens primair zijn vastgelegd in de Wpg en de Wjsg.

Tegelijkertijd, zo blijkt uit paragraaf 5.4.1 en 5.4.2 van deze wetgevingstoets, worden via het voorliggende concept belangrijke bepalingen betreffende het bewaren, vernietigen en doelafwijkend gebruik van met strafvorderlijke bevoegdheden verzamelde persoonsgegevens opnieuw in het nieuwe Wetboek van Strafvordering opgenomen. De AP adviseert de gekozen wetgevingssystematiek nader te doordenken.

Voor zover verschillende wetten vergelijkbare onderwerpen regelen, mag over de verhouding tussen beiden geen misverstand bestaan. Daarom moet uit de tekst van de wet of op zijn minst ondubbelzinnig uit de toelichting op het nieuwe Wetboek van Strafvordering duidelijk blijken hoe de desbetreffende bepalingen in het nieuwe wetboek zich verhouden tot de bestaande bepalingen in de Wpg en de Wjsg. Zo moet naar het oordeel van de AP duidelijk zijn dat de (strengere) bepaling over het doelafwijkend gebruik van met opsporingsbevoegdheden verzamelde persoonsgegevens in het nieuwe wetboek (zie voorgestelde artikel 2.1.20) een *lex specialis* is van het aanzienlijk ruimer en algemener geformuleerde artikel 9, derde lid, Wpg dat gaat over het doelafwijkend gebruik van politiegegevens die gericht worden verwerkt “ten

¹¹⁶ HvJEU 21 december 2016 C-203/15 ECLI:EU:C:2016:970 (*Tele2 Sverige*), punt 121; *Landeck*, ECLI:EU:C:2024:830, punt 118-121, *Ligue des droits humains* ECLI:EU:C:2023:874, punt 58-59, *Ministerstvo na vatreshnite raboti*, ECLI:EU:C:2023:49, punt 89.

¹¹⁷ Arikelen 24a en 24b van de Wpg.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

behoefte van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval'. Hetzelfde geldt voor de verhouding van de bepalingen inzake het bewaren en vernietigen van persoonsgegevens in het nieuwe wetboek (zie voorgestelde artikelen 2.1.18 en 2.1.19) tot de artikelen in de Wpg die gaan over het verwijderen en vernietigen van politiegegevens die worden verwerkt in het kader van een opsporingsonderzoek (artikel 9, vierde lid en artikel 14 Wpg).

5.5 Overige opmerkingen ten aanzien van het concept

Bevoegdheid tot het heimelijk inloggen in een geautomatiseerd werk (artikel 2.8.17)

Het concept bevat een nieuwe bevoegdheid die ertoe strekt dat een opsporingsambtenaar heimelijk en op afstand kan binnendringen in een digitale-gegevensdrager of een geautomatiseerd werk, door in te loggen met de – in de rechtmatige uitoefening van zijn bediening verkregen - inloggegevens van de gebruiker daarvan. Deze nieuwe bevoegdheid maakt het mogelijk om vanaf de vaste werkplek van de ambtenaar met de verkregen inloggegevens in te loggen op bijvoorbeeld een cloud-omgeving, sociale media of op het email-account van de verdachte. Uit de toelichting blijkt dat het gaat om inloggegevens die beschikbaar zijn gekomen bij toepassing van andere bevoegdheden. Te denken valt aan een onderzoek aan een inbeslaggenomen mobiele telefoon, of een gevonden notitieboekje met inloggegevens tijdens een doorzoeking.

De AP merkt op dat heimelijk mogen inloggen terecht onderworpen is aan hoge eisen, zoals machtiging van de rechter-commissaris en het criterium van een ernstige inbreuk op de rechtsorde. Dat geldt echter niet voor de herkomst van de te benutten inloggegevens; alle inloggegevens waarover de opsporingsambtenaar beschikt 'in de rechtmatige bediening van zijn functie' mogen worden gebruikt voor toepassing van deze bevoegdheid. Naast het voorbeeld van een doorzoeking die inloggegevens oplevert, noemt de toelichting in dit verband ook gegevens die verzameld zijn op basis van artikel 3 Politiewet. Dat betekent dat ook inloggegevens uit een geheel andere context dan het opsporen van ernstige misdrijven (de uitvoering van de dagelijkse politietaken waaronder ook de handhaving van de openbare orde valt) in aanmerking komen voor heimelijk gebruik. Uit de wetstekst blijkt daarbij niet dat het moet gaan om inloggegevens van verdachten zodat ook inloggegevens van personen die in het geheel niet zijn betrokken bij criminele feiten in beginsel heimelijk benut kunnen worden.

Om misbruik van bevoegdheden ter verkrijging van inloggegevens tegen te gaan, is de AP is van oordeel dat de voorafgaande toetsing door de rechter-commissaris die voor de inzet van deze bevoegdheid is vereist, ook zou moeten omvatten een toets of de inloggegevens inderdaad door een opsporingsambtenaar 'in de rechtmatige uitoefening van de bediening' zijn verkregen en de opsporingsambtenaar deze bovendien nog steeds rechtmatig onder zich heeft. Dat de machtiging van de rechter-commissaris ook dit aspect moet dekken, dient naar het oordeel van de AP uit de tekst van de wet of uit de toelichting te blijken.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

6. Werklast AP

In de memorie van toelichting bij het voorstel voor vaststellingswet I is opgemerkt dat het nieuwe Wetboek van Strafvordering grote implicaties voor de uitvoering zal hebben.¹¹⁸ Dit blijkt ook uit paragraaf 14 van de toelichting bij het voorliggende concept. Mede gelet op al hetgeen in deze wetgevingstoets is opgenomen en zeker wanneer het nationale strafprocesrecht uit de pas blijft lopen met het Europese gegevensbeschermingsrecht, acht de AP het een gegeven dat het concept de AP zal nopen tot substantiële extra inzet voor de uitvoering van haar toezichthoudende en voorlichtende taken. Deze inzet is nog niet verdisconteerd in de financiering van de AP. Dit zal voorafgaand aan inwerkingtreding in overleg met de Staatssecretaris Rechtsbescherming - als verantwoordelijk bewindspersoon voor de begroting ten laste waarvan de AP wordt gefinancierd - moeten worden geadresseerd. Om die reden verzoek ik de Staatssecretaris dan ook de inhoud van deze wetgevingstoets ook in dat kader te betrekken.

7. Openbaarmaking

Deze wetgevingstoets wordt twee weken na dagtekening op de website van de AP gepubliceerd.

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter

¹¹⁸ Kamerstuk II 2022/23, 36 327, nr. 3, p. 73.



Datum
3 maart 2025

Ons kenmerk
z2024-014439

Bijlage

Toetsingskader AP

De AP beziet of het concept met betrekking tot de verwerking van persoonsgegevens strookt met het Handvest van de Grondrechten van de Europese Unie (EU), de AVG (Verordening 2016/679) of de Richtlijn Gegevensbescherming Rechtshandhaving (richtlijn 2016/680), de algemene rechtsbeginselen van de EU en het overige relevante recht, waarbij onder meer voldoende aannemelijk moet zijn gemaakt dat voldaan wordt aan het evenredigheidsbeginsel, doordat:

1. het concept geschikt is om de nagestreefde doelstelling van algemeen belang of de bescherming van de rechten en vrijheden van anderen te verwezenlijken (*geschiktheid*);
2. het doel niet redelijkerwijs even doeltreffend kan worden bereikt op een andere wijze, die de grondrechten van de betrokkenen minder aantast (*subsidiariteit*);
3. de inmenging niet onevenredig is aan dat doel, wat met name een afweging impliceert van het belang van het doel en de ernst van de inmenging (*proportionaliteit*);
4. het concept voldoende duidelijk en nauwkeurig is over de reikwijdte en in de toepassing voorspelbaar is (*rechtszekerheid*);
5. het concept voldoende aangeeft in welke omstandigheden en onder welke voorwaarden persoonsgegevens kunnen worden verwerkt, en aldus waarborgt dat de inmenging tot het strikt noodzakelijke wordt beperkt (*inhoudelijke en procedurele waarborgen*) en
6. het concept verbindend is naar nationaal recht (*verbindendheid naar nationaal recht*).

De AP slaat daarbij in het bijzonder acht op de rechten van betrokkenen en de overeenstemming van het concept met artikel 6, eerste en derde lid, en 9, van de AVG, dan wel 8 en 10 van de Richtlijn Gegevensbescherming Rechtshandhaving en met de in artikel 5 van de AVG dan wel artikel 4 van de Richtlijn vastgestelde beginselen. Hieruit volgt onder andere dat:

- (a) verwerkingen *rechtmatig, behoorlijk en transparant* moeten zijn ten aanzien van de betrokkene;
- (b) dat persoonsgegevens alleen mogen worden verzameld voor *welbepaalde, nadrukkelijk omschreven en gerechtvaardigde doeleinden*; en
- (c) verwerkingen *toereikend zijn, ter zake dienend en beperkt moeten zijn tot wat voor de doeleinden noodzakelijk is*.