Modernisering strafvordering en de bescherming van persoonsgegevens in het opsporingsonderzoek

Schermer, B.W.; Custers, B.H.M.

B.W. Schermer & B.H.M. Custers[1]

Artikelen

Modernisering strafvordering en de bescherming van persoonsgegevens in het opsporingsonderzoek[2]

DD 2024/45

In deze bijdrage gaan wij in op de verhouding tussen opsporingsbelangen en privacy bij (grootschalige) gegevensverwerkingen. Centraal staat de verhouding tussen het huidige Wetboek van Strafvordering en het Wetsvoorstel Vaststelling van het nieuwe Wetboek van Strafvordering enerzijds en de Wet politiegegevens anderzijds. Wij betogen dat deze verhouding problematisch is vanwege de 'harde knip' tussen beide regelingen. Wij pleiten voor een meer geïntegreerde benadering waarbij de waarborgen voor de bescherming van persoonsgegevens tijdens het verzamelen en verder verwerken van gegevens beter op elkaar worden afgestemd.

1. Inleiding

In 2020 waren maar liefst 60.000 mensen geabonneerd op EncroChat, een Europese aanbieder van een communicatienetwerk met aangepaste smartphones.[3] De meeste gebruikers waren bezig met georganiseerde criminaliteit en hadden een netwerk als EncroChat nodig om buiten beeld van de autoriteiten te blijven. In het voorjaar van 2020 infiltreerde de politie in het netwerk en legde het plat.[4] Tegen het eind van dat jaar waren meer dan duizend mensen gearresteerd.[5]

Digitaal bewijs speelt een steeds belangrijkere rol in opsporingsonderzoeken. Enerzijds is dat het gevolg van een toename van cybercriminaliteit: als criminaliteit zich in toenemende mate online afspeelt, zal ook de opsporing grotendeels online moeten plaatsvinden. Anderzijds is dat het gevolg van technologische en maatschappelijke ontwikkelingen waarbij steeds meer mensen, dus ook criminelen, gebruik maken van steeds geavanceerdere technologie. Dus ook als de criminaliteit geen vorm van cybercrime is, wordt er vaak wel gecommuniceerd via technologische netwerken, al dan niet versleuteld zoals in het geval van EncroChat.

Elke vorm van digitale communicatie laat in beginsel digitale sporen achter. Hoewel het op elektronische communicatienetwerken (telefoon, whatsapp, e-mail, videobellen, etc.) zeer eenvoudig is om anoniem te blijven en berichten te versleutelen, blijven er niettemin sporen achter die bruikbaar kunnen zijn in opsporingsonderzoeken. Met toenemende bijzondere opsporingsmethoden, bijvoorbeeld het opvragen van gegevens bij providers, het doorbreken van beveiliging en het 'terughacken' van criminelen, kunnen verdere

1 *Prof. mr. dr. B.W. (Bart) Schermer is hoogleraar Privacy & Cybercrime bij eLaw, het Centrum voor Recht en Digitale Technologie aan de Universiteit Leiden en partner bij adviesbureau Considerati. Prof. mr. dr. ir. B.H.M. (Bart) Custers is hoogleraar Law and Data Science en directeur van eLaw, het Centrum voor Recht en Digitale Technologie aan de Universiteit Leiden.*

2 Citeerwijze: B.W. Schermer & B.H.M. Custers, 'Modernisering strafvordering en de bescherming van persoonsgegevens in het opsporingsonderzoek', DD 2024/45.

3 R. Stoykova, 'Encrochat: The hacker with a warrant and fair trials?', *Forensic Science International: Digital Investigation* 2023/46.

4 R. Kennedy, 'EU authorities penetrate phone network in huge organised crime sting', *Euronews*, 2 juli 2020.

5 R. Wright, 'Hundreds arrested across Europe as French police crack encrypted network' *The Financial Times,* 2 juli 2020.

aanknopingspunten en aanwijzingen in opsporingsonderzoeken worden verkregen.[6] Die informatie kan later ook dienen als bewijsmateriaal in de rechtszaal.
De hoeveelheden gegevens die online worden verstuurd zijn enorm. In een opsporingsonderzoek wordt slechts een deel daarvan afgevangen, maar doorgaans zijn dat nog steeds grote hoeveelheden gegevens. Als er op grote schaal gegevens worden verzameld, zitten daar ook persoonsgegevens bij, niet alleen van verdachten, maar ook van anderen. De gegevens kunnen bovendien zeer gevoelig zijn. Als bijvoorbeeld gegevens worden verkregen via een hack door politie (zoals bij EncroChat), inbeslagname van smartphones, het vorderen van gegevens, of samenwerking met andere autoriteiten (bijvoorbeeld de FIU of buitenlandse autoriteiten), kan daar van alles tussen zitten. Door de toenemende mogelijkheden van de beschikbare analysemethoden (data analytics zoals Hansken van het NFI)[7] kan bovendien verdergaand inzicht worden verkregen in de persoonlijke levenssfeer van mensen. Het op grote schaal verzamelen en analyseren van gegevens heeft een impact op de persoonlijke levenssfeer van betrokkenen en kan hun privacy en bescherming van persoonsgegevens schenden. Zeker voor degenen die geen verdachte zijn in een opsporingsonderzoek (inclusief slachtoffers en getuigen) kan dit schadelijk zijn, maar ook verdachten in een opsporingsonderzoek hebben bepaalde rechten ten aanzien van hun privacy en de bescherming van hun persoonsgegevens. Ook kunnen de gegevens van bijvoorbeeld advocaten onderdeel vormen van een dataset waardoor het verschoningsrecht onder druk kan komen te staan.
Kortom, de belangen van een opsporingsonderzoek en de rechten van betrokkenen kunnen tegenover elkaar staan in dergelijke situaties. Deze bijdrage gaat in op de vraag hoe de verhouding tussen deze belangen geregeld is, zowel in de huidige regeling als in het Wetsvoorstel Vaststelling van het nieuwe Wetboek van Strafvordering, en waar nog tekortkomingen zitten die mogelijk moeten worden geadresseerd.[8] Daarbij wordt ingegaan op de twee regelingen waarin de bescherming van persoonsgegevens in opsporingsonderzoeken momenteel primair is geregeld: in het Wetboek van Strafvordering (WvSv) en de Wet politiegegevens (Wpg). Het Wetboek van Strafvordering gaat vooral over het rechtmatig *verzamelen* van gegevens (in het bijzonder daar waar het gaat om het verzamelen van gegevens met behulp van opsporingshandelingen waarbij een meer dan geringe inbreuk wordt gemaakt op de persoonlijke levenssfeer), de Wet politiegegevens gaat over het *gebruik* van gegevens die door de politie rechtmatig zijn verzameld. Daar waar het gaat om de verwerking van persoonsgegevens door het OM is de Wet justitiële en strafvordelijke gegevens (Wjsg) van toepassing.[9]
Deze bijdrage is als volgt opgebouwd. Paragraaf 2 gaat in op het recht op privacy en het recht op bescherming van persoonsgegevens. Paragraaf 3 beschrijft de regeling in het Wetboek van Strafvordering, vooral gericht op het verzamelen van gegevens. Paragraaf 4 doet hetzelfde voor de Wet politiegegevens, vooral gericht op het gebruik van gegevens. Paragraaf 5 beschrijft het samenspel tussen beide regelingen, of beter gezegd, het gebrek

6 R.L.D. Pool & B.H.M. Custers, 'The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime', *European Journal of Crime, Criminal Law and Criminal Justice,* 2017/25, p. 123-144.
7 H.M.A. van Beek, J. van den Bos, A. Boztas, E.J. van Eijk, R. Schramp, M. Ugen, 'Digital forensics as a service: Stepping up the game', *Forensic Science International: Digital Investigation*, 2020/35.
8 Vaststelling van het nieuwe Wetboek van Strafvordering (Wetboek van Strafvordering), *Kamerstukken II* 2022/23, 36 327, nr. 2 (Voorstel van wet).
9 Gegeven de omvang van deze bijdrage zullen wij ons beperken tot een bespreking van de verhouding tussen het Wetboek van Strafvordering en de Wet politiegegevens. Voor een bespreking van de normering van de verwerking van strafrechtelijke gegevens zie: R.A. Hoving, *Verwerking van strafrechtelijke gegevens door het openbaar ministerie*, Den Haag: Boom Juridisch 2022 en W.L. Borst, 'Naar een gegevenswet voor het strafrechtelijk domein?', *DD* 2024/27, p. 360-379.

daaraan. Paragraaf 6 biedt voorstellen voor de verdere ontwikkeling van een gebalanceerde regeling. Paragraaf 7 rondt af met conclusies.

2. Privacy en gegevensbescherming

Het recht op bescherming van de persoonlijke levenssfeer (de privacy) is in diverse mensenrechtenverdragen zoals het IVBPR (artikel 17) en het EVRM (artikel 8) vastgelegd. In onze Grondwet worden in de artikelen 10 t/m 13 Grondwet de diverse aspecten van de persoonlijke levenssfeer beschermd.
De bescherming van persoonsgegevens (de informationele privacy) vormt een steeds belangrijker aspect van onze persoonlijke levenssfeer. De bescherming van persoonsgegevens vormt binnen de context van het EVRM een onderdeel van het privé-, familie- en gezinsleven (artikel 8 EVRM).[10] In de Nederlandse Grondwet en het Handvest Grondrechten van de Europese Unie is de bescherming van persoonsgegevens vormgegeven als een zelfstandig recht (respectievelijk artikel 10 lid 2 Grondwet en artikel 8 HGEU).
Persoonsgegevens die in de uitvoering van de politietaak worden verwerkt worden politiegegevens genoemd (zie artikel 1 onder a Wpg). Artikel 1 onder b Wpg definieert een persoonsgegeven als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene).[11]
De bescherming van persoonsgegevens kan op verschillende manieren in het geding komen door de toepassing van opsporingsbevoegdheden. Zo is de bescherming van persoonsgegevens in het geding wanneer de politie een gegevensdrager in beslag neemt met daarop gevoelige gegevens over de betrokkene. De bescherming van persoonsgegevens kan ook in het geding komen wanneer een digitale tap wordt geplaatst. Met behulp van de tap wordt inbreuk gemaakt op het communicatiegeheim (artikel 13 Grondwet), maar tegelijkertijd worden ook persoonsgegevens verwerkt.
Door het verzamelen van persoonsgegevens wordt dus een inbreuk gemaakt op de persoonlijke levenssfeer. Tegelijkertijd wordt het verwerken van deze gegevens steeds belangrijker voor de opsporing. Denk hierbij aan het combineren van gegevenssets en (geautomatiseerde) analyse van gegevens met behulp van kunstmatige intelligentie. Het Europees Hof voor de Rechten van de Mens (EHRM) concludeert in de arresten *Big Brother Watch e.a. t. Verenigd Koninkrijk* en *Centrum för Rättvista t. Zweden* dat de grootste inbreuken op de privacy in de analysefase plaatsvinden.[12] Ook het Hof van Justitie van de Europese Unie is van mening dat de analysefase aparte waarborgen moet kennen.[13] In relatie tot de grootschalige verwerking van Encrochat gegevens overwoog de rechtbank Midden-Nederland dat juist in de fase van het verwerken van de data de mate van inbreuk op artikel 8 EVRM het grootst is.[14]

10 Europees Hof voor de Rechten van de Mens, *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, versie 9 april 2024.
11 Gegeven het wijdverbreide gebruik van het begrip persoonsgegeven, ook binnen de opsporing, hanteren wij in dit artikel de term 'persoonsgegeven' in plaats van 'politiegegeven'.
12 EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a.* t. *Verenigd Koninkrijk*); EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för rättvista t. Zweden*). Voor een bespreking zie: M. Galič, 'Bulkbevoegdheden en strafrechtelijk onderzoek: lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse', *Tijdschrift voor Bijzonder Strafrecht en Handhaving* 2022, nr. 3.
13 HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258 (*Commissioner of An Garda Síochána*); HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*), *NJ* 2022/140.
14 Rb. Midden-Nederland 12 april 2022, ECLI:NL:RBMNE:2022:1423.

Inbreuken op het privé-, familie- en gezinsleven moeten op grond van artikel 8 EVRM bij wet zijn voorzien. Naarmate de inbreuk op de grondrechten van burgers (potentieel) groter is, is een meer robuuste wettelijke regeling noodzakelijk aldus het EHRM. Deze regeling moet ten minste duidelijkheid geven over de volgende elementen:

- de aard, de omvang en de duur van de maatregel;
- de gronden op basis waarvan de maatregel gevorderd kan worden;
- de autoriteiten die bevoegd zijn om de maatregel toe te staan, uit te voeren en te toetsen.[15]

Deze wettelijke regeling wordt in Nederland primair geboden door het Wetboek van Strafvordering en de Wet politiegegevens. Tussen deze twee regelingen bestaat volgens de wetgever een 'harde knip'.[16] Deze harde knip komt er kort gezegd op neer dat de *verzameling* van persoonsgegevens tijdens het opsporingsonderzoek genormeerd wordt door het Wetboek van Strafvordering, terwijl het daaropvolgende *gebruik* van de gegevens door de politie binnen het opsporingsonderzoek wordt genormeerd door de Wet Politiegegevens.[17] Onderstaand bespreken wij eerst beide regelingen afzonderlijk alvorens wij ingaan op de synergie (of het gebrek daaraan) tussen deze twee regelingen.

3. Het verzamelen van gegevens: het Wetboek van Strafvordering

Het Wetboek van Strafvordering biedt van oudsher de wettelijke basis voor rechtmatige inbreuken op de privacy tijdens de opsporing. Het wetboek geeft aan ten behoeve van welke doelen en onder welke omstandigheden een bevoegdheid mag worden ingezet. Ook biedt het wetboek waarborgen, onder andere in de vorm van de *ex ante* en *ex post* rechterlijke toetsing van de opsporing. De mate van inbreuk op het recht op privacy en de invloed daarvan op het recht op een eerlijk proces is daarbij maatgevend.
Voor geringe inbreuken volstaat artikel 3 Politiewet jo artikel 141 Sv als wettelijke basis, maar wanneer er een meer dan geringe inbreuk op de persoonlijke levenssfeer wordt gemaakt, dan moet daarvoor een specifieke wettelijke regeling zijn.[18] Deze regelingen zijn te vinden in het Wetboek van Strafvordering, in het bijzonder in de regelingen rondom de inbeslagname en de bijzondere opsporingsbevoegdheden.

Met het wetsvoorstel Vaststelling van het nieuwe Wetboek van Strafvordering (verder: NSv) wordt deze opzet geherstructureerd en gestroomlijnd.[19] Allereerst komt er een nieuwe algemene 'basisbevoegdheid' tot opsporing voor de politie in de vorm van artikel 2.1.9 NSv:

15 Zie: EHRM (GK) 6 september 1978, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass e.a. t. Duitsland)*; EHRM 29 juni 2006 ECLI:CE:ECHR:2006:0629DEC005493400 (*Weber en Saravia t. Duitsland)*; EHRM (GK) 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov t. Rusland*), *NJ* 2017/185, m.nt. E.J. Dommering.

16 *Kamerstukken II* 2022/23, 36 327, nr. 3, p. 70 (memorie van toelichting).

17 De opvolger van de Wpg (en Wjsg) die ambtelijk bekend staat als 'de gegevensbeschermingwet' of 'integrale gegevenswet' werd voor onbepaalde tijd uitgesteld. Zie: Memorie van toelichting bij de Wet politiegegevens, *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 3; Brief van 29 maart 2022, *Kamerstukken II* 2021/22, 32 761 en 33 842, nr. 218, p. 2. Dat van uitstel afstel komt blijkt uit de memorie van toelichting bij het Voorstel van wet tot vaststelling van het nieuwe Wetboek van Strafvordering. Op pagina 71 wordt gemeld dat de gegevensbeschermingswet er niet komt.

18 Zie onder andere: HR 19 december 1995, ECLI:NL:HR:1995:ZD0328 (*Zwolsman arrest*), *NJ* 1996/249, m.nt. T.M. Schalken en HR 4 april 2017, ECLI:NL:HR:2017:584 (*Smartphone arrest*), *NJ* 2017/229, m.nt. T. Kooijmans.

19 *Kamerstukken II* 2022/23, 36 327, nr. 2 (voorstel van wet).

> "Opsporingsambtenaren zijn ter uitvoering van hun taak bevoegd om in overeenstemming met de geldende rechtsregels onderzoekshandelingen te verrichten."

Voor de meer ingrijpende inbreuken komt er een specifieke regeling voor de inbeslagname en het onderzoek aan gegevensdragers (Boek 2, hoofdstuk 7 NSv) en een regeling voor de heimelijke bevoegdheden (Boek 2, hoofdstuk 8 NSv), die grofweg overeenkomt met de huidige bijzondere opsporingsbevoegdheden. Naast het stroomlijnen van de bestaande bijzondere opsporingsbevoegdheden wordt een tweetal nieuwe bevoegdheden voorgesteld: het stelselmatig overnemen van gegevens uit openbare bronnen en het stelselmatig bepalen van de locatie van een persoon. Verder is met betrekking tot de toegang op afstand tot geautomatiseerde werken (de 'hackbevoegdheid') geregeld dat gegevens uit deze geautomatiseerde werken mogen worden overgenomen om de waarheid aan het licht te brengen (2.8.16 NSv). Daar waar het gaat om het onderzoeken van de inbeslaggenomen gegevens stelt artikel 2.7.38 NSv het volgende:

> "Stelselmatig onderzoek van gegevens in een digitale-gegevensdrager of geautomatiseerd werk of ten aanzien van gegevens die daaruit zijn overgenomen, kan door een opsporingsambtenaar alleen op bevel van de officier van justitie worden verricht."

De wetgever formuleert hier een nieuw criterium voor de beoordeling van de aard en de ernst van de inbreuk op de persoonlijke levenssfeer: de stelselmatigheid. De wetgever maakt een onderscheid tussen 'onderzoek' (niet als zodanig gedefinieerd), 'stelselmatig onderzoek' en 'ingrijpend stelselmatig onderzoek'. Stelselmatig onderzoek is in artikel 2.1.1 NSv gedefinieerd als:

> "Een onderzoek van gegevens waarbij op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan."

De Commissie Koops merkt op dat het juridische begrip stelselmatig niet overeenkomt met het begrip 'stelselmatig' zoals we dat in het normale spraakgebruik hanteren.[20] Het gaat niet zozeer om de herhaling van de handeling, maar veeleer om het gevolg van de handeling: het verkrijgen van een bepaald beeld van de persoon. Naast het stelselmatig onderzoek van gegevens is er het 'ingrijpend stelselmatig onderzoek'. Ingrijpend stelselmatig onderzoek is gereguleerd in artikel 2.7.38 lid 2 NSv:

> "In geval van ingrijpend stelselmatig onderzoek kan het bevel alleen worden gegeven indien het belang van het onderzoek dit dringend vereist en na een daartoe verleende machtiging van de rechter-commissaris."

Een ingrijpend stelselmatig beeld kan volgens de memorie van toelichting bij het moderniseringsvoorstel ontstaan wanneer er een min of meer volledig beeld van een wezenlijk deel van iemands privéleven wordt verkregen (diepe kijk) en/of een min of meer volledig beeld van een aanzienlijk deel van iemands privéleven (brede kijk).[21] Omdat er bij een ingrijpend stelselmatig onderzoek sprake is van een potentieel zeer vergaande privacy inbreuk, is de tussenkomst van een onafhankelijke rechterlijke autoriteit noodzakelijk.

20 Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018 (Commissie Koops), p. 194.

21 *Kamerstukken II* 2022/23, 36 327, nr. 3, (memorie van toelichting), p. 575.

Wat moet worden aangetekend is dat het begrip 'stelselmatig' géén algemeen normeringscriterium is. De begrippen 'stelselmatig' en 'ingrijpend stelselmatig' zijn in het nieuwe wetboek specifiek gekoppeld aan de regeling van het onderzoek aan gegevensdragers. Dit is enigszins verwarrend, omdat de term stelselmatig ook gebezigd wordt in de context van het stelselmatig onderzoek naar gegevens uit openbare bronnen. Bij dit gebruik van het woord stelselmatig moeten we waarschijnlijk wél uitgaan van de betekenis in het normale spraakgebruik. Voor het bepalen van de mate van inbreuk van het stelselmatig overnemen van gegevens uit openbare bronnen worden in de memorie van toelichting separate criteria aangedragen.[22]

3.1 *Waarborgen*

Wanneer het verzamelen van persoonsgegevens niet bij wet is voorzien of niet plaats heeft op de wijze bij wet voorzien (een vormverzuim in de zin van artikel 359a Sv), dan kan dit consequenties hebben voor het recht op een eerlijk proces zoals beschermd door artikel 6 EVRM. Dit zou bijvoorbeeld het geval kunnen zijn wanneer de gegevens op een geheime wijze zijn verzameld en de verdediging niet in staat is om de accuraatheid van de gegevens en de rechtmatigheid van de verzameling te toetsen.
Overigens betekent een schending van artikel 8 EVRM niet onmiddellijk dat de beginselen van een goede procesorde zijn geschaad.[23] Wanneer een schending van artikel 8 EVRM niet van wezenlijke invloed is op het verloop van het proces, dan hoeven daar van de Hoge Raad geen rechtsgevolgen aan te worden verbonden.[24] Het is uiteindelijk de vraag of de procedure als geheel eerlijk is aldus het EHRM.[25] Relevante aspecten bij de beoordeling of er sprake is van een inbreuk op het recht op eerlijk proces zijn onder andere de rol die het bewijs speelt in de veroordeling,[26] de betrouwbaarheid van het bewijs,[27] het bestaan van procedurele waarborgen en de mogelijkheden van de verdediging om het bewijs te toetsen[28] en het handelen van de autoriteiten bij het verzamelen van het bewijs.[29]
Overtreding van de strafvorderlijke regels kan op grond van artikel 359a Sv strafvorderlijke consequenties hebben. Dit is een stevige waarborg voor de bescherming van privacy en persoonsgegevens in de vorm van de *ex post* rechterlijke toetsing. Hierbij moet wel worden aangetekend dat de lat voor zware sancties zoals bewijsuitsluiting hoog ligt.

In zijn arrest van 1 december 2020 heeft de Hoge Raad aangegeven in welke situaties bewijsuitsluiting een passende sanctie is.[30] Allereerst is er de situatie waarin bewijsuitsluiting noodzakelijk is om het recht op een eerlijk proces te waarborgen. Daarnaast kan het in uitzonderlijke gevallen noodzakelijk zijn om tot bewijsuitsluiting te komen als *"rechtsstatelijke waarborg en als middel om met de opsporing en vervolging belaste ambtenaren te*

22 *Kamerstukken II* 2022/23, 36 327, nr. 3, (memorie van toelichting), p. 679 e.v.
23 EHRM 12 mei 2000, ECLI:CE:ECHR:2000:0512JUD003539497, (*Khan t. Verenigd Koninkrijk*), *NJ* 2002/180, m.nt. T.M. Schalken.
24 HR 7 juli 2009, ECLI:NL:HR:2009:BH8889, *NJ* 2009/399.
25 EHRM 12 juli 1988, ECLI:CE:ECHR:1988:0712JUD001086284 (*Schenk t. Zwitserland*); EHRM 12 mei 2000, ECLI:CE:ECHR:2000:0512JUD003539497 (*Khan t. Verenigd Koninkrijk*), *NJ* 2002/180, m.nt. Schalken.
26 EHRM 10 maart 2009, ECLI:CE:ECHR:2009:0310JUD000437802 (*Bykov t. Rusland*); EHRM (GK) 1 juni 2010, ECLI:CE:ECHR:2010:0601JUD002297805 (*Gäfgen t. Duitsland*), *NJ* 2010/628, m.nt. Y. Buruma.
27 EHRM 26 september 2023, ECLI:CE:ECHR:2023:0926JUD001566920 (*Yüksel Yalçınkaya t. Turkije*)
28 EHRM 26 september 2023, ECLI:CE:ECHR:2023:0926JUD001566920 (*Yüksel Yalçınkaya t. Turkije*); EHRM 10 maart 2009, ECLI:CE:ECHR:2009:0310JUD000437802 (*Bykov t. Rusland*).
29 Is er bijvoorbeeld sprake geweest van dwang, misleiding of manipulatie (EHRM 5 februari 2003, ECLI:CE:ECHR:2002:1105JUD004853999 (*Allan t. Verenigd Koninkrijk*), *NJ* 2004/262).
30 HR 1 december 2020, ECLI:NL:HR:2020:1889, *NJ* 2021/169, m.nt. N. Jörg. Zie ook: HR 19 september 2023, ECLI:NL:HR:2023:1264.

weerhouden van onrechtmatig optreden en daarmee als middel om te voorkomen dat vergelijkbare vormverzuimen in de toekomst zullen plaatsvinden".[31] Daarbij moet aldus de Hoge Raad *"acht worden geslagen op de negatieve effecten die aan bewijsuitsluiting zijn verbonden, gelet op de zwaarwegende belangen van waarheidsvinding, van de vervolging en berechting van (mogelijk zeer ernstige) strafbare feiten, en in voorkomend geval van de rechten van slachtoffers."*[32]

Naast de *ex post* toetsing door de zittingsrechter is er de *ex ante* toetsing door een (rechterlijke) autoriteit in de vorm van een bevel van de officier van justitie en de machtiging van de rechter-commissaris. Tabel 1 toont een overzicht van de bevoegdheden in het huidige en het nieuwe Wetboek van Strafvordering waarbij per bevoegdheid is aangegeven welke autoriteit bevoegd is om het bevel te geven.[33]

Bevoegdheid	**Nieuw artikel**	**Huidig artikel**
Stelselmatige observatie	2.8.7 *	126g *
Stelselmatig overnemen persoonsgegevens uit publiek toegankelijke bronnen	2.8.8 *	-
Bevoegdheden ten aanzien van een besloten plaats	2.8.9 *	126k *
Pseudo-koop of dienstverlening	2.8.10 *	126i *
Stelselmatige inwinning van informatie	2.8.11*	126j *
Infiltratie	2.8.12 *	126h *
Vastleggen communicatie die plaatsvindt door middel van een aanbieder van een communicatiedienst	2.8.13 **	126m **
Vastleggen vertrouwelijke communicatie	2.8.16 **	126l **
Toegang op afstand tot een digitale-gegevensdrager of geautomatiseerd werk	2.8.17 **	126nba **
Stelselmatige locatiebepaling	2.8.18 *	-

Tabel 1: Overzicht van de bevoegdheden WvSv en NSv (= officiersbevoegdheid, ** = machtiging rechter-commissaris)*

Met betrekking tot de *ex ante* (rechterlijke) toetsing is de jurisprudentie van het Hof van Justitie van de Europese Unie relevant.[34] In het bekende *Prokuratuur* arrest heeft het Hof besloten dat het vorderen van verkeersgegevens alleen mag plaatsvinden na goedkeuring door een rechterlijke autoriteit of onafhankelijk bestuursorgaan.[35] De *Prokuratuur* jurisprudentie heeft alleen betrekking op het vorderen van verkeersgegevens. Maar het lijkt erop dat het Hof de redenering uit *Prokuratuur* gaat doortrekken naar het onderzoek aan gegevens uit inbeslaggenomen gegevensdragers. In de zaak *C.G. tegen Bezirkshauptmannschaft Landeck,* die ten tijde van het schrijven van deze bijdrage aanhangig is bij het HvJEU, overweegt de A-G in ieder geval dat de politie niet op eigen initiatief en zonder tussenkomst

31 HR 1 december 2020, ECLI:NL:HR:2020:1889, *NJ* 2021/169, m.nt. Jörg, r.o. 2.4.4.
32 HR 1 december 2020, ECLI:NL:HR:2020:1889, *NJ* 2021/169, m.nt. Jörg, r.o. 2.4.4.
33 Wij beperken ons hier tot de bevoegdheden uit Boek 2, hoofdstuk 8 NSv. Boek 2, hoofdstuk 7 NSv bevat naast de inbeslagname ook de regels rondom het vorderen van gegevens.
34 Merk op dat er soms nogal een kloof zit tussen de Nederlandse praktijk en het Handvest. Bovendien kan de jurisprudentie nogal meanderen, zie P. Verrest, 'De invloed van het Handvest op het Nederlandse strafrecht', in: J.H. Gerards e.a., *Waarde, werking en potentie van het EU-Grondrechtenhandvest in de Nederlandse rechtsorde. Preadviezen* (*Handelingen Nederlandse Juristen-Vereniging 153e jaargang*) Deventer: Wolters Kluwer 2024, p. 139-209.
35 HvJ EU, 2 maart 2021, C-746/18, ECLI:EU:C:2021:152. Zie ook: HR 5 april 2022, ECLI:NL:HR:2022:475, *NJ* 2022/354, m.nt J.W. Ouwerkerk.

van een rechter of onafhankelijk bestuursorgaan, volledige en ongecontroleerde toegang mag krijgen tot in beslag genomen gegevens.[36] Hoewel beargumenteerd kan worden dat toegang die niet 'volledig en ongecontroleerd' is dus wel mogelijk is zonder toestemming van een rechterlijke autoriteit, ligt een dergelijke lezing niet voor de hand. Dit betekent dat het voor het verzamelen van persoonsgegevens volgens de A-G bij het Hof altijd een onafhankelijke toetsing noodzakelijk is. Aangezien in Nederland de officier van justitie aan het hoofd van het onderzoek staat, lijkt een bevel van de officier daarom niet te volstaan. Het feit dat de officier aan het hoofd van het onderzoek staat maakt het moeilijk om vol te houden dat deze onafhankelijk is in de procedure.

4. Het verwerken van gegevens: de Wet politiegegevens

De Wet politiegegevens dateert van 2008 en verving toen de Wet politieregisters. Naar aanleiding van EU-richtlijn 2016/680 (Law Enforcement Directive, LED)[37] is de Wet politiegegevens herzien. Wat betreft opzet en structuur lijkt de LED op de Algemene verordening gegevensbescherming (AVG).[38] Beide regelingen werden in 2016 tegelijkertijd gepubliceerd. De LED kan worden gezien als een *lex specialis* van de AVG. Maar terwijl de AVG als verordening direct bindend is, diende de LED eerst geïmplementeerd te worden in nationale wetgeving. In Nederland vond dit plaats door de Wpg (en de Wet justitiële en strafvorderlijke gegevens, Wjsg) te herzien. De aangepaste Wpg is sinds 1 januari 2019 van kracht.
De reikwijdte van de Wpg wordt bepaald door de begrippen politiegegeven en bevoegde autoriteit (art. 2 Wpg). Politiegegevens zijn alle persoonsgegevens die worden verwerkt in het kader van de uitvoering van de politietaak (art. 1 sub a Wpg). Persoonsgegevens zijn, net als in de AVG, gedefinieerd als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1 sub b Wpg). Anonieme gegevens, gegevens van rechtspersonen en gegevens van overledenen vallen buiten het bereik van deze definitie.

Bevoegde autoriteiten zijn alle overheidsinstanties die bevoegd zijn 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 (art. 1 subl l Wpg). Lidstaten kunnen ook andere entiteiten aanwijzen als bevoegde autoriteit. In Nederland zijn alle onderdelen van de strafrechtketen, waaronder uiteraard politie en OM, in elk geval bevoegde autoriteiten. De Koninklijke Marechaussee is een bevoegde autoriteit voor zover het haar politietaken betreft.
Als de politie in het kader van een opsporingsonderzoek bijvoorbeeld persoonsgegevens vordert van bedrijven, dan vallen diezelfde gegevens bij het betreffende bedrijf onder de AVG, maar bij de politie onder de Wpg. Het zijn weliswaar dezelfde gegevens, maar ze worden voor andere doeleinden gebruikt. Politiegegevens mogen slechts worden verwerkt voor de in de Wpg genoemde doelen (art. 3 Wpg). Dat zijn de doelen die bevoegde autoriteiten

36 Conclusie van Advocaat-Generaal M. Campos Sánchez-Bordona van 20 april 2023, Zaak C-548/21, ECLI:EU:C:2023:313 (*C.G. tegen Bezirkshauptmannschaft Landeck*).

37 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016, 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 van de Raad (*PbEU* L 119/89).

38 Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016, betreffende de bescherming van natuurlijke personen in verband met de verwerking persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (*PbEU* L 119/1).

definiëren, dus preventie, onderzoek, opsporing en vervolging van strafbare feiten alsook tenuitvoerlegging van straffen.
Algemene uitgangspunten in art. 3 Wpg zijn dat de politiegegevens slechts mogen worden verwerkt voor zover dit behoorlijk en rechtmatig is, de gegevens rechtmatig zijn verkregen, toereikend, ter zake dienend en niet bovenmatig zijn gelet op de doelen waarvoor ze worden gebruikt. Art. 4 Wpg voegt daaraan toe dat de politie verantwoordelijk is voor de juistheid en nauwkeurigheid van de gegevens. Onjuiste gegevens moeten worden gerectificeerd of verwijderd. Gegevens die niet volledig of up-to-date zijn, moeten worden aangevuld en geactualiseerd. Een lastige bepaling is artikel 4 lid 3 Wpg, dat stelt dat de politie zoveel mogelijk moet onderscheiden wat feiten danwel persoonlijke oordelen betreft. Dit is ingewikkeld, omdat dit onderscheid niet altijd even helder is.[39]
Andere verplichtingen voor de politie zijn het zorgen voor voldoende beveiliging van de gegevens (art. 4a en 4b), het uitvoeren van impact assessments om risico's in te schatten (art. 4c), extra bescherming van gevoelige gegevens (art. 5), een systeem van autorisaties onderhouden (art. 6) en de geheimhoudingsplicht (art. 7). De artikelen 8 tot en met 10 Wpg gaan verder in op verschillende doeleinden waarvoor politiegegevens kunnen worden verwerkt. Artikel 8 Wpg ziet op de uitvoering van de dagelijkse politietaak. Artikel 9 Wpg ziet op het verwerken van politiegegevens in het kader van meer omvangrijke opsporingsonderzoeken of verkennende onderzoeken. Artikel 10 Wpg ziet ten slotte op het verwerken van politiegegevens teneinde meer inzicht te krijgen in ernstige misdrijven en terroristische activiteiten.
Al deze bepalingen stellen voorwaarden aan het verzamelen en verwerken van politiegegevens. Maar in de Wpg is er maar één bepaling omtrent het analyseren van gegevens. Dat is artikel 11 Wpg. Artikel 11 Wpg is gericht op het geautomatiseerd vergelijken van politiegegevens, teneinde vast te stellen of er verbanden zijn. Ook kunnen de gegevens worden vergeleken met niet-politiebestanden en open bronnen. De beperking van art. 11 Wpg zit erin dat enkel in het kader van een concreet opsporingsonderzoek (als in de artikelen 9 en 10 Wpg) geautomatiseerde data-analyse mag worden toegepast. In het kader van de algemene politietaak (art. 8 Wpg) mag geen geautomatiseerde gegevensvergelijking worden toegepast. Artikel 11 Wpg is de enige bepaling die data-analyse reguleert, maar doet dat op een weinig concrete manier. Over andere vormen van data-analyse dan geautomatiseerde gegevensvergelijking wordt helemaal niets gezegd. Geautomatiseerde data-analyse lijkt in alle vormen toegestaan, zolang dit ten doel staat van de opsporing. Dit is een onwenselijke situatie om verschillende redenen.
Ten eerste zijn er inmiddels zeer geavanceerde analysemethoden beschikbaar die vergaande details uit de persoonlijke levenssfeer kunnen achterhalen dan wel voorspellen.[40] Op basis van summiere informatie kunnen zo zeer gevoelige gegevens worden achterhaald. Bijvoorbeeld op basis van een postcode kunnen al opleidingsniveau, inkomen, etniciteit en gezinssamenstelling worden voorspeld. Op basis van online gedragingen kunnen zeer gevoelige aspecten zoals seksuele oriëntatie, etniciteit, politieke voorkeuren en drugsgebruik worden voorspeld.[41] Kortom, geavanceerde analysemethoden kunnen veel verdergaande inbreuken op de privacy veroorzaken dan op het eerste gezicht mogelijk lijkt.

39 B.H.M. Custers & M.R. Leiser, 'Persoonsgegevens in het strafrecht: weeffouten in EU-richtlijn 2016/680 leiden tot praktische problemen', *NJB* 2019, afl. 34, p. 2490-2497.

40 B.H.M. Custers, 'Big Data in wetenschappelijk onderzoek', *Justitiële Verkenningen*, 2016/1, p. 8-21.

41 M. Kosinski, D. Stillwell, T. Graepel, 'Private Traits and Attributes are Predictable from Digital Records of Human Behaviour', *Proceedings of the National Academy of Sciences USA* 2012/110, p. 5802–5805. De voorspellingen kunnen vervolgens als aannames worden gebruikt in opsporingsonderzoeken en ook in dossiers voor opsporing en vervolging terechtkomen, waar ze een eigen leven kunnen gaan leiden.

Ten tweede kunnen de analysemethoden discriminerende effecten vertonen. Uit onderzoek is bekend dat voorspelmodellen gebruikt in het strafrecht discriminerend kunnen zijn. In delen van de Verenigde Staten leunen rechters op het recidive-voorspelmodel COMPAS.[42] Dit model, hoewel niet openbaar, bleek systematisch Afro-Amerikanen hogere recidiverisico's toe te kennen.[43]
Ten derde, daaraan gerelateerd, is het voor betrokkenen bij dit soort modellen doorgaans zeer lastig dan wel onmogelijk om de modellen en de conclusies die daaruit voortvloeien te verifiëren of te betwisten. Zelfs als de modellen geen intellectueel eigendom zijn (en daarmee een 'black box'), is het doorgaans lastig voor betrokkenen om te volgen welke input leidt tot welke output. De modellen zijn doorgaans zeer complex en in het geval van zeer geavanceerde analysemethoden (zoals kunstmatige intelligentie, AI) ook zelflerend. Daardoor kunnen de modellen verder evolueren en is elk begrip van "deze input leidt tot deze conclusie" slechts een momentopname. De grote hoeveelheden data die worden gebruikt om de modellen te trainen zijn niet met menselijke intuïtie en inzichten te doorzien (daarvoor zijn deze instrumenten in de eerste plaats nodig).
Ten vierde, het gebrek aan transparantie en inzicht in hoe de geavanceerde analyses werken, kan ertoe leiden dat het niet wordt rechtgezet als er verkeerde conclusies worden getrokken. Door het ontbreken van correctiemechanismen bestaat het risico op fouten. Onjuiste conclusies kunnen weliswaar worden betwist in de rechtszaal, maar dat is buitengewoon lastig als niet duidelijk is hoe de analysemethoden werken en hoe de conclusies tot stand komen. Er ontstaat bovendien een soort omgekeerde bewijslast waarbij een betrokkene moet uitleggen waarom de modellen of analyseresultaten niet kloppen, hetgeen spanning met het onschuldbeginsel oplevert. Degenen die de modellen bouwen of analyses uitvoeren hebben daardoor een veel stevigere positie, waarbij *equality of arms* niet altijd kan worden gegarandeerd.[44]

5. Het samenspel tussen het WvSv en de Wpg (of het gebrek daaraan)

Op basis van het voorgaande kunnen we concluderen dat het WvSv en de Wpg twee complementaire systemen zijn die gezamenlijk het recht op privacy, het recht op gegevensbescherming én het recht op een eerlijk proces moeten borgen. Het WvSv normeert de verzameling van de gegevens, de Wpg richt zich primair op het verder verwerken van de gegevens binnen de politieorganisatie. Hoewel de Nederlandse wetgever in de memorie van toelichting bij het moderniseringsvoorstel een 'harde knip' maakt tussen het verzamelen en verder verwerken, blijkt uit onder andere de redactie van de LED en de Wpg dat deze knip niet zo hard is als wordt voorgesteld door de wetgever.[45] Zo strekken de LED en de Wpg zich ook uit tot de verzamelfase. Het begrip 'verwerken van gegevens' omvat namelijk ook het verzamelen van de gegevens (zie artikel 3 onder 2 LED en artikel 1 onder c Wpg). Dit betekent dat de rechtmatigheid van het verzamelen van persoonsgegevens niet alleen wordt genormeerd door het WvSv, maar ook door de LED en de Wpg.[46]

42 Zie: https://njoselson.github.io/pdfs/FieldGuide2_081412.pdf.
43 J. Angwin, J. Larson, S. Mattu, L. Kirchner, 'Machine Bias', *ProPublica*, 23 mei 2016.
44 B.H.M. Custers, 'Technologiekennis voor een eerlijk proces: fair trial vereist ook van rechters enige kennis van complexe technologie', *NJB* 2023/21, p. 1733-1741.
45 Ditzelfde geldt overigens ook voor de Wjsg. Zie Borst 2024.
46 Zie ook: HR 3 juli 2012, ECLI:NL:HR:2012:BV1800.

Andersom zien we dat het WvSv ook de verwerking normeert. Hirsch Ballin signaleert dat het opsporingsbegrip qua reikwijdte met de tijd ruimer en diffuser is geworden.[47] Zo bevindt de preventieve inzet van digitale analysetechnieken ter voorkoming van strafbare feiten zich in het grensgebied van de opsporing en valt het daarmee binnen de kaders van de Politiewet, de Wpg én het Wetboek van Strafvordering.[48] De hierboven beschreven bevoegdheid tot inbeslagname van gegevensdragers uit het nieuwe Wetboek van Strafvordering normeert óók het onderzoek aan deze gegevens, in ieder geval daar waar het gaat om het toestaan van de bevoegdheid.[49] Momenteel wordt de bevoegdheid tot het onderzoeken van gegevens uit in beslag genomen voorwerpen in de huidige artikelen 95 en 96 WvSv gelezen.[50] Ook in andere bepalingen uit het WvSv kan een bevoegdheid tot verwerken worden gelezen, aldus de rechter. Zo stelt de rechtbank Midden-Nederland dat de hackbevoegheid (thans artikel 126uba WvSv) ook de analyse van de gegevens omvat:

> "(…) dat het geautomatiseerde werk kan worden doorzocht en dat in het belang van het onderzoek gegevens of gegevensbestanden kunnen worden vastgelegd. Dit is niet beperkt tot de gegevens die zijn opgeslagen, maar kan ook betrekking hebben op gegevens die na het tijdstip van afgifte van het bevel worden opgeslagen. Artikel 126uba Sv biedt dus de mogelijkheid om een geautomatiseerd werk te hacken, de data op te slaan en te analyseren met als doel om die data in een strafrechtelijke procedure te gebruiken."[51]

Verder stellen de artikelen 126cc, 126dd en 126ee WvSv regels met betrekking tot het vernietigen van gegevens die zijn verzameld met behulp van bijzondere opsporingsbevoegdheden en het doorgeven ervan aan andere onderzoeken. Met name deze laatste bepaling speelt in samenhang met de artikelen uit de Wpg een grote rol in het overhevelen van gegevens van het ene onderzoek naar het andere.
Deze bepalingen bieden weliswaar een juridische basis voor het verwerken en bepalen welke autoriteiten bevoegd zijn om de toepassing van de bevoegdheid te gelasten, maar bieden verder geen regels voor het uitvoeren van de analyse. Er wordt dus maar in beperkte mate tegemoet gekomen aan de vereisten gesteld door het EHRM, meer specifiek de voorzienbaarheid, zoals besproken in paragraaf 2. Dit roept de vraag op of de huidige wijze waarop gegevens worden verwerkt wel voldoende bij wet is voorzien. Dit is zorgelijk, omdat in steeds meer onderzoeken gegevens in bulk worden verzameld en verder verwerkt. In bijvoorbeeld de EncroChat en SkyECC onderzoeken is dit het geval.
In één van de vele 'EncroChat zaken' heeft de verdediging zich onder andere op het standpunt gesteld dat de verwerking van 'bulkdata' door de politie niet bij wet is voorzien en daarom een effectieve rechtsbescherming ontbreekt.[52] De verdediging haalt daarbij onder andere de LED aan. De rechtbank verwerpt dit verweer en verwijst daarbij naar de beantwoording van de prejudiciële vragen over EncroChat door de Hoge Raad. Kort gezegd komt het argument van de rechtbank erop neer dat omdat de Hoge Raad geen voorschriften zag in de LED die relevant waren voor de beoordeling van de prejudiciële vragen, de rechtbank ook niet hoeft in te gaan op het verweer van de verdediging.[53]

47 M.F.H. Hirsch Ballin, *Responsief strafprocesrecht in een netwerk van rechtsbetrekkingen*, preadvies Christen Juristen Vereniging, Zutphen: Uitgeverij Paris 2022, p. 22.
48 Hirsch Ballin 2022, p. 21.
49 Zie Boek 2 Hoofdstuk 7 NSv.
50 HR 4 april 2017, ECLI:NL:HR:2017:584, *NJ* 2017/229, m.nt. T. Kooijmans.
51 Rb. Midden-Nederland 12 april 2022, ECLI:NL:RBMNE:2022:1423.
52 Rb. Den Haag 15 augustus 2023, ECLI:NL:RBDHA:2023:12353.
53 Rb. Den Haag 15 augustus 2023, ECLI:NL:RBDHA:2023:12353.

De prejudiciële vragen die door de Hoge Raad zijn beantwoord, hebben nagenoeg allemaal betrekking op de toepassing van het interstatelijk vertrouwensbeginsel.[54] Alleen de zevende prejudiciële vraag van de rechtbank Noord-Nederland (zie r.o. 4.2) gaat over de rechtmatigheid van de verdere verwerking:

> "Is een wettelijke grondslag vereist voor het bewaren en gebruiken van de metadata en communicatie van gebruikers van een elektronische communicatiedienst door de Nederlandse autoriteiten, ten behoeve van de opsporing en vervolging van strafbare feiten, als deze is verkregen van een andere lidstaat, nadat die andere lidstaat deze data heeft geïntercepteerd?"[55]

Met betrekking tot de rol van de LED volstaat de Hoge Raad in zijn antwoord met het aangeven dat de LED relevant is wanneer (persoons)gegevens in Nederland worden verwerkt ten behoeve van de opsporing of vervolging. De Hoge Raad overweegt (in r.o. 6.27.4) dat de LED verder geen voorschriften bevat die specifiek van belang zijn voor de beantwoording van de prejudiciële vragen. Met name de toevoeging van de zinssnede "*als deze is verkregen van een andere lidstaat, nadat die andere lidstaat deze data heeft geïntercepteerd*" lijkt de vraag toe te spitsen op de rechtmatigheid van de verzameling, niet op de rechtmatigheid van de analyse. Als de Hoge Raad de vraag inderdaad als zodanig heeft begrepen, dan behoeft de LED inderdaad geen verdere bespreking. Immers, op grond van het vertrouwensbeginsel mogen we ervan uitgaan dat de Fransen zich aan de regels van de LED hebben gehouden.
Wanneer wij het verweer van de verdediging begrijpen als dat er onderzoek moet worden gedaan naar het feit of het handelen van de Franse opsporingsautoriteiten in strijd is geweest met de LED, omdat de bulkverzameling niet bij wet is voorzien en niet voldoet aan het vereiste van evenredigheid, dan is het oordeel van de rechtbank begrijpelijk. Het interstatelijk vertrouwensbeginsel staat immers in de weg aan een dergelijk onderzoek door de Nederlandse rechter. Echter, wanneer wij het verweer van de verdediging begrijpen als dat voor de opvolgende verwerking door de Nederlandse politie geen rechtsgrond bestaat, omdat de analyse van de bulkdata onvoldoende voorzienbaar is, dan wordt het een ander verhaal. Dan volstaat het niet langer om te verwijzen naar de prejudiciële vragen van de Hoge Raad, omdat de Hoge Raad in zijn antwoorden niet in de beoordeling van deze situatie is getreden. Helaas lijkt de rechtbank het verweer te hebben begrepen als een aanval op de rechtmatigheid van de verzameling, waardoor een antwoord op de prangende vraag of (bulk)data-analyse voldoende bij wet is voorzien voorlopig uitblijft.
Rechters lijken sowieso terughoudend in het toetsen van de opsporing aan de vereisten uit de LED en de Wpg.[56] In tal van EncroChat zaken heeft de verdediging bijvoorbeeld betoogd dat de verwerkingen in strijd zijn met de Richtlijn en tevergeefs verzocht prejudiciële vragen te stellen aan het Hof van Justitie van de Europese Unie over de toepassing van de LED in relatie tot bulkverzameling en -analyse.[57] De rechtbank Gelderland ging zelfs zo ver om te stellen dat de Wpg geen strafvorderlijk relevante voorschriften bevat en als zodanig er geen strafvorderlijke consequenties aan de overtreding ervan hoeven te worden verbonden.[58]

54 Voor een analyse zie: J.J. Oerlemans, B.W. Schermer, 'Antwoorden op prejudiciële vragen in de EncroChat- en SkyECC-zaken', *NJB* 2023/31, p. 2610-2618.
55 Hoge Raad 13 juni 2023, ECLI:NL:HR:2023:913, *NJ* 2023/279, m.nt. J.M. Reijntjes, r.o 4.2.
56 Custers 2023.
57 Zie bijvoorbeeld: Rb. Amsterdam 8 juli 2021; ECLI:NL:RBAMS:2021:3524; Rb. Amsterdam 15 februari 2022, ECLI:NL:RBAMS:2022:568 en Hof 's-Hertogenbosch 25 april 2022, ECLI:NL:GHSHE:2022:1387. Hierbij moet worden aangetekend dat het primair ging om vragen over de verzamelfase die in het kader van Encrochat grotendeels buiten schot blijft in verband met het interstatelijk vertrouwensbeginsel.
58 Rb. Gelderland 28 april 2021, ECLI:NL:RBGEL:2021:2277.

Wie in een concreet opsporingsonderzoek zijn hoop vestigt op de Wpg voor effectieve rechtsbescherming komt waarschijnlijk ook bedrogen uit. Zoals wij hebben beschreven in paragraaf 4 biedt de Wpg weinig tot geen concrete vereisten voor de rechtmatige verwerking van gegevens, anders dan vereisten die zijn gericht op de zorgvuldige omgang met de gegevens zoals bijvoorbeeld de beveiliging van de gegevens en bewaartermijnen. Een bijkomend probleem is dat de Autoriteit Persoonsgegevens de naleving van de bepalingen uit de Wpg weliswaar toetst, maar daarbij nooit in een beoordeling van de rechtmatigheid van de gegevensverwerking in een concreet opsporingsonderzoek treedt.[59] Ook kan zij geen strafvorderlijke consequenties verbinden aan normoverschrijdingen mocht zij overtredingen van de Wpg constateren.[60]

Op basis van het bovenstaande kunnen we concluderen dat concrete regels en effectief toezicht op de analyse van gegevens ten behoeve van de opsporing grotendeels ontbreekt. In zoverre het WvSv een grondslag biedt voor het verder verwerken van de gegevens, zijn de daarvoor geldende regels niet opgenomen in het WvSv zelf en lijken rechters (vooralsnog) terughoudend te zijn in het toetsen van de verwerkingen van persoonsgegevens aan de eisen zoals gesteld door het EHRM, de LED en de Wpg. Daar waar het gaat over de toetsing van de naleving van de Wpg zien we dat de AP zich niet bemoeit met de rechtmatigheid van een verwerking in een concreet geval. De rechtsbescherming dreigt daarmee tussen wal en schip te vallen.[61]

Deze situatie is naar onze mening in strijd met de vereisten die het EHRM stelt aan de verzameling en analyse van (bulk)gegevens. Het EHRM heeft in de arresten *Big Brother Watch e.a. t. Verenigd Koninkrijk* en *Centrum för Rättvista t. Zweden* aangegeven dat een nationale wettelijke regeling voor bulkinterceptie en -analyse tenminste duidelijkheid moet bieden over de volgende aspecten:

1. De gronden waarop bulkinterceptie kan worden toegestaan;
2. De omstandigheden waarin de communicatie van een individu kan worden onderschept;
3. De te volgen procedure voor het verlenen van toestemming;
4. De te volgen procedures voor het selecteren, onderzoeken en gebruiken van onderschept materiaal;
5. De voorzorgsmaatregelen die moeten worden genomen bij het communiceren van het materiaal aan andere partijen;
6. Grenzen aan de duur van de verzameling, de opslag van het materiaal en de omstandigheden waarin dergelijk materiaal moet worden gewist en vernietigd;
7. De procedures en modaliteiten voor toezicht door een onafhankelijke autoriteit op de naleving van de bovengenoemde waarborgen en haar bevoegdheden om niet-naleving aan te pakken;
8. De procedures voor onafhankelijke toetsing achteraf van deze naleving en de toegekende bevoegdheden bij de bevoegde instantie die gevallen van niet-naleving aanpakt.[62]

59 B.W. Schermer & M. Galič, 'Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?' *Nederlands Tijdschrift voor Strafrecht* 2022/38, p. 167-177.

60 M. Fedorova, R. te Molder, M. Dubelaar, S. Lestrade, T. Walree, *Strafvorderlijke gegevensverwerking, een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Nijmegen: Radboud University Press 2022, p. 33.

61 B.W. Schermer, *De gespannen relatie tussen privacy en cybercrime* (oratie Universiteit Leiden), 7 november 2022.

62 EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a.* t. *Verenigd Koninkrijk*); EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för rättvista t. Zweden*).

Wanneer wij kijken naar het WvSv en Wpg als een samenhangend systeem, dan zien we dat dit systeem (voor wat betreft de analysefase) momenteel tekortschiet op met name de punten 3, 4, 7 en 8.

6. Hoe nu verder?

Op basis van het bovenstaande concluderen wij dat de huidige inrichting van het wettelijk systeem ontoereikend is en twee primaire zwaktes kent:

1) Hoewel voor het verzamelen van (bulk)gegevens duidelijke strafvorderlijke regels bestaan, ontbreken deze regels grotendeels voor de analyse van gegevens.
2) De strafvorderlijke waarborgen en sancties die het WvSv kent voor de verzamelfase ontbreken voor de analysefase, omdat deze fase wordt genormeerd door de Wpg.

Fedorova e.a. hebben in hun WODC-rapport een aantal suggesties gedaan voor het verbeteren van de normering. Vanuit wetssystematisch perspectief stellen zij voor verwerkingshandelingen die zijn gericht op kennisvermeerdering én een strafvorderlijk doel dienen in het WvSv onder te brengen en aldaar nader te normeren. Zo wordt recht gedaan aan het uitgangspunt dat het WvSv de inzet en uitoefening van opsporingsmethoden normeert, zoals dat ook voortvloeit uit het strafvorderlijk legaliteitsbeginsel.[63] Wij onderschrijven deze aanpak, niet in de laatste plaats omdat het daarmee helder(der) wordt dat het overtreden van de normen strafvorderlijke consequenties kan hebben. Fedorova e.a. stellen voor om een nieuwe titel te creëren in Boek 2 NSv die de algemene regels voor gegevensanalyse omschrijft.[64] Daarnaast zouden specifieke regels kunnen worden opgesteld voor bulkverzameling en analyse van gegevens.[65] Daarbij moet in het bijzonder aandacht worden besteed aan duidelijke regels en procedures voor het selecteren, onderzoeken en gebruiken van het materiaal.
Hoewel steeds meer auteurs en instanties de mening zijn toegedaan dat de huidige en voorgestelde toekomstige kaders ontoereikend zijn, lijken oplossingen zoals die door onder andere Fedorova e.a. zijn voorgesteld vooralsnog niet in zicht.[66] Bij de parlementaire behandeling van Boek 2 NSv hebben de leden van de CDA-fractie (nogmaals) hun zorgen geuit over het uitblijven van de modernisering van de Wpg.[67] Maar vooralsnog is het plan om tot een integrale gegevenswet te komen in de ijskast geplaatst.[68] In plaats daarvan schuift de wetgever het probleem voor zich uit door te stellen dat de richting waarin de normering zich zou moeten begeven nog niet altijd precies vast te stellen is.[69]

63 Fedorova e.a. 2022, p. 157 e.v.
64 Fedorova e.a. 2022, p. 160.
65 Fedorova e.a. 2022, p. 161.
66 Zie voor een overzicht van deze auteurs en instanties: L. Stevens e.a., *Inhoudelijke rapportage Boek 2: Het opsporingsonderzoek*, Project bijstand Tweede Kamer modernisering Wetboek van Strafvordering, p. 10; en meest recentelijk: L. Stevens, 'Alle ballen op het OM? Over wie verantwoordelijk is voor normering van en toezicht op onderzoek aan (grote hoeveelheden) digitale data', *DD* 2024/26, p. 353-359.
67 *Kamerstukken II* 2023/2024, 36 327, nr. 6, p. 4.
68 Merk op dat de eerste aanvullingswet nieuwe Wetboek van Strafvordering erkent dat modernisering van de Wpg uitblijft, maar gaat wel een aantal bepalingen (126cc en 126dd Sv) opnemen in het nieuwe wetboek die waren geschrapt. Zie https://www.internetconsultatie.nl/aanvullingswet/b1.
69 *Kamerstukken II* 2022/23, 36 327, nr. 3, (memorie van toelichting), p. 71.

7. Conclusie

De grootschalige verzameling, opslag en analyse van gegevens wordt steeds belangrijker in de opsporing. Om een goede balans te vinden tussen het belang van de opsporing, het recht op privacy en het recht op een eerlijk proces, zijn regels voor het verzamelen en verder verwerken van politiegegeven vastgelegd in het WvSv en de Wpg. Dit systeem voorziet echter onvoldoende in een helder juridisch kader dat voldoende bescherming biedt voor de burger. We concluderen dat de tekortkomingen in het huidige systeem hun oorsprong hebben in het gebrek aan samenhang tussen de twee wettelijke kaders die gegevensverwerking binnen de opsporing normeren (het WvSv en de Wpg). Omdat in de opsporing het verzamelen en analyseren nauw met elkaar verweven zijn, ligt het voor de hand om één gemeenschappelijk kader te creëren voor het gebruik van gegevens binnen de opsporing. In plaats daarvan heeft de wetgever in het moderniseringsvoorstel de 'harde knip' tussen het WvSv en de Wpg nogmaals bevestigd. Hopelijk komt de wetgever terug op dit standpunt en komt er een regeling die recht doet aan de eisen zoals gesteld door het EHRM en het EU Hof van Justitie.