M.F.H. Hirsch Ballin & J.J. Oerlemans[1]

Artikel

Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden[2]

DD 2023/2

In dit artikel wordt de praktijk van datagedreven opsporing beschreven en worden de consequenties ervan voor het stelsel van strafvordering geduid. Om datagedreven opsporing uit normatief oogpunt in te bedden in het stelsel van strafvordering, zal moeten worden onderkend dat de toepassing van opsporingsbevoegdheden óók gericht kan zijn op andere doelstellingen (zoals het verstoren van criminele infrastructuren of het produceren van intelligence). Daarbij moeten worden gezocht naar een vorm van normering die ook passend is voor deze andere doelstellingen. Het is daarvoor noodzakelijk dat het Wetboek van Strafvordering en de Wet politiegegevens beter op elkaar aansluiten en het stelsel van toezicht en controle op datagedreven opsporing opnieuw wordt ingericht.

1. Inleiding

Datagedreven opsporing is de verwerking van gegevens die eerder door de politie bij hun taakuitoefening in andere onderzoeken zijn verzameld en daarna ten behoeve van nieuwe opsporingsonderzoeken worden geanalyseerd. Deze datagedreven opsporing moet worden onderscheiden van het gebruik van data vergaard door andere (private of overheids)instanties en van het gebruik van uitkomsten van data-analyses door andere (overheids)instanties die aan de politie of het openbaar ministerie worden verstrekt ten behoeve van de opsporing.[3] Alhoewel het ook hier gaat om datagedreven opsporing, richten wij ons in deze bijdrage op het gebruik van data verkregen door de politie bij de eigen taakuitoefening. De zogenoemde 'cryptotelefoon-operaties' zijn een bekend voorbeeld van deze datagedreven opsporing. Daarbij zijn tot wel honderden miljoenen berichten in één operatie veiliggesteld van cryptotelefoonaanbieders zoals 'EncroChat' en 'Sky ECC'. Deze gegevens vormen (ten dele) bewijs voor honderden toekomstige strafzaken. Datagedreven opsporing kan daarmee worden beschouwd als een 'game changer' voor de politiepraktijk.[4]

Door onderzoek aan deze grote hoeveelheden gegevens krijgt de politie meer zicht op criminele organisaties en strafbare feiten. De gegevens zijn van grote waarde in opsporingsonderzoeken en dragen bij om grip te krijgen op de zware georganiseerde criminaliteit (het betreft in de woorden van het hoofd van de Landelijke Recherche Andy Kraag: *"een*

---

1 *Prof. dr. mr. M.F.H. Hirsch Ballin is hoogleraar Straf- en strafprocesrecht aan de Vrije Universiteit Amsterdam. Daarnaast is zij advocaat bij Pels Rijcken. Prof. mr. dr. J.J. Oerlemans is bijzonder hoogleraar Inlichtingen en recht aan de Universiteit Utrecht. Daarnaast is hij senioronderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).*

2 Citeerwijze: M.F.H. Hirsch Ballin & J.J. Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijke optreden', *DD* 2023/2.

3 Zie over de normering van data-analyses door de NCTV en het (toekomstige) Multidisciplinaire Interventieteam/Nationale Samenwerking tegen Ondermijnende Criminaliteit (MIT/NSOC) en het gebruik van de uitkomsten ervan voor (onder meer) de opsporing: M.F.H. Hirsch Ballin, 'Als een spin in het web voor de bestrijding van terrorisme en zware ondermijnende criminaliteit', *TvCr* 2022, 2, p. 1-26 (hierna: Hirsch Ballin 2022-1).

4 Stoker, E., 'Politie kon wekenlang meelezen met geheime berichten van duizenden zware criminelen', *De Volkskrant*, 2 juli 2020.

goudmijn aan bewijs").[5] Ook wij zijn ervan overtuigd dat door het analyseren van beschikbare gegevens de middelen van de politie en het Openbaar Ministerie efficiënter en effectiever kunnen worden ingezet en strafbare feiten sneller kunnen worden opgespoord. De methode is inmiddels in de rechtspraak geregeld getoetst. In de rechtspraak waar bewijs vergaard door de cryptotelefoon-operaties een rol heeft gespeeld, hebben die operaties de toets van de strafrechter doorstaan.[6] De Hoge Raad kwam bijvoorbeeld in het arrest van 28 juni 2022 tot het oordeel dat de van de Canadese autoriteiten verkregen Ennetcom-gegevens en het gebruik daarvan voor een Nederlandse strafzaak na een machtiging van de rechter-commissaris rechtmatig was.[7] Daarbij moet niettemin worden opgemerkt – zoals we verderop nader zullen toelichten – dat de beoordeling van de strafrechter niet als een volledige inhoudelijke beoordeling van de methode van 'datagedreven opsporing' kan worden beschouwd. De methode staat desondanks dan ook nog steeds, zowel in Nederland als in het buitenland, ter discussie.[8] Daarnaast is de methode in de rechtspraak getoetst in het licht van het recht op een eerlijk proces (en het beginsel van 'gelijke rechtsmiddelen') en lijkt dat in deze zaken in beginsel voldoende te worden gewaarborgd.[9] De rechtmatigheid van de verzameling van de gegevens in de cryptotelefoonzaken en de vragen met betrekking tot het recht op een eerlijk proces zullen we in deze bijdrage verder buiten beschouwing laten.

De vraag of het Wetboek van Strafvordering, in samenhang met de bepalingen van de Wet politiegegevens (hierna: Wpg), voldoende normering biedt voor datagedreven opsporing gaat verder dan de beoordeling van de strafrechter in het licht van het toetsingskader op grond van artikel 359a Sv. In de eerste plaats verdient de verhouding tussen de bevoegdheid tot verzameling van de gegevens – op grond van bepalingen in het Wetboek van Strafvordering en op grond van de politietaak ex artikel 3 Politiewet 2012 – en de bevoegdheid tot

5 *Ibid.*

6 Zie voor een overzicht van de rechtspraak met betrekking tot EncroChat: B.W. Schermer & J.J. Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?', *TBS&H* 2022, 2, p. 82-89 (hierna: Schermer & Oerlemans 2022).

7 HR 28 juni 2022, ECLI:NL:HR:2022:900, r.o. 3.5.1-3.6.6.

8 Zie ook de 'brandbrief strafrechtadvocatuur over gekraakte chatberichten' van 24 oktober 2022. In een persbericht van 4 november 2022 maakte het OM bekend dat de Rechtbank Noord-Nederland (uitspraak niet gepubliceerd) voornemens is prejudiciële vragen te stellen aan de Hoge Raad over de beoordeling van de rechtmatigheid van het gebruik van berichten uit de EncroChat- en Sky ECC-zaken. In Italië oordeelde de Corte di Cassazione op 15 juli 2022 (strafrechtelijk vonnis Kamer 4, nr. 32915 jaar 2022) dat bekend moet worden gemaakt op welke wijze het bewijs is vergaard en ander bewijs moet worden uitgesloten, omdat dit in strijd zou zijn met artikel 6 EVRM. In Frankrijk en Duitsland spelen vergelijkbare zaken. De Court de Cassation oordeelde op 11 oktober 2022 (nr. 01226, ECLI:FR:CCASS:2022:CR01226) dat de bewijsverzameling in EncroChat-zaken beter uitgelegd en gemotiveerd moet worden en het Landsgericht Berlin stelde prejudiciële vragen aan het Hof van Justitie van de Europese Unie (LG Berlijn Beschl. 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22)).

9 Zie HR 28 juni 2022, ECLI:NL:HR:2022:900, r.o. 3.5.1-3.6.6 met betrekking tot de verzameling van gegevens van cryptotelefoonprovider Ennetcom en r.o. 4.4.1-4.6 over het recht op inzage met betrekking tot de verzamelde en verwerkte gegevens. Zie ook HR 8 maart 2022, ECLI:NL:PHR:2022:219, concl. A-G Harteveld. Zie verder ook S.G.A.M. Adams, 'Vertrouwen is goed, maar controle is beter. De interpretatie van het interstatelijke vertrouwensbeginsel door Nederlandse feitenrechter bij samenwerking tussen EVRM-lidstaten in het kader van internationale digitale rechtshulp in strafzaken en het beginsel van equality of arms', *DD* 2021/74 (hierna: Adams 2021), M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *BoomStrafblad* 2021/2, D.N. de Jonge & S.L.J. Janssen, 'Eindelijk toegang tot datasets. (Erg) langzaam maar zeker naar een nieuw normaal', *NJB* 2021/2532 en de reactie daarop van J.C. van der Pijll, 'De dataset langs de meetlat van artikel 6 EVRM', *NJB* 2022/291 en M.M. Egberts, 'De reikwijdte van het inzagerecht en 'equality of arms' in het licht van grote datasets, Hansken en toekomstige ontwikkelingen', *TBS&H* 2022/2.6 (hierna: Egberts 2022) en J.J. Oerlemans & D.A.G. van Toor, 'Legal Aspects of the EncroChat Operation: A Human Rights Perspective', *European Journal of Crime, Criminal Law and Criminal Justice* 2022, p. 310–329.

verdere verwerking en analyse – op grond van de bepalingen van de Wpg aandacht. Het gaat er daarbij om dat, in het bijzonder vanuit het perspectief van het recht op bescherming van de persoonlijke levenssfeer, een gescheiden benadering van de normering niet houdbaar lijkt.[10] Voorts is de vraag of de normering op grond van de Wpg volstaat gelet op de vereisten die voorvloeien uit de rechtspraak van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) en het Hof van Justitie van de Europese Unie (hierna: HvJ EU).[11] Deze punten zijn inmiddels in de literatuur al geregeld aan bod gekomen en staan in onze bijdrage dan ook niet centraal. Datagedreven opsporing is daarnaast, in de tweede plaats, een praktijk die vergt dat in bredere zin wordt beoordeeld hoe die zich verhoudt tot de doelstellingen en uitgangspunten van het strafprocesrecht.

In dit artikel richten wij ons op het tweede punt en dus op de vraag of de methode van datagedreven onderzoek – het verdere gebruik van gegevens in andere onderzoeken en voor andere doeleinden dan het onderzoek waarin die gegevens zijn verkregen – uit normatief oogpunt is in te bedden in het bestaande strafvorderlijke kader. Het gaat ons daarbij om de verhouding tussen de doelstellingen van de datagedreven opsporing en de doelstellingen en uitgangspunten van het stelsel van strafvordering, in het bijzonder gelet op het daaraan verbonden systeem van toezicht en controle.

Het artikel is als volgt opgebouwd. Paragraaf 2 schetst de ontwikkeling van het concept van datagedreven opsporing aan de hand van de beleidstheorie die is ontwikkeld door het team High Tech Crime en aan de hand van voorbeelden uit de praktijk. In paragraaf 3 zetten wij uiteen welke bepalingen de grondslag (worden geacht te) vormen voor deze datagedreven opsporing. Vervolgens leggen wij in paragraaf 4 en 5 uit waarom het concept van datagedreven opsporing leidt tot spanningen in relatie tot de uitgangspunten van ons huidige stelsel van strafvordering. Wij beogen hiermee inzichtelijk te maken dat datagedreven opsporing druk legt op de huidige uitgangspunten van het stelsel van strafvordering. De consequentie daarvan is ook dat weinig ruimte bestaat voor controle door de strafrechter op de rechtmatigheid van het (volledige) proces van datagedreven opsporing. Paragraaf 6 gaat om deze reden nader in op het toezicht en de controle op datagedreven opsporing. Ten slotte geven wij in paragraaf 7 een oplossingsrichting mee voor een betere inbedding van de praktijk van datagedreven opsporing in het grensgebied van strafvordering en gegevensbeschermingsrecht en bieden wij een daarbij aansluitende andere benadering van het toezicht op de praktijk.

2. Het concept van datagedreven opsporing

Het Team High Tech Crime van de Nationale Politie heeft het concept van ‘datagedreven opsporing’ in de afgelopen jaren daadwerkelijk tot wasdom gebracht. In een paper getiteld ‘Towards Data Scientific Investigations: A Comprehensive Data Science Framework

10 Zie daarover: M.F.H. Hirsch Ballin, *Responsief strafprocesrecht in een netwerk van rechtsbetrekkingen,* preadvies CJV 2022, beschikbaar via: http://christenjuristen.nl/wp-content/uploads/2022/09/Preadvies-CJV-Marianne-Hirsch-Ballin-20220914.pdf.

11 Zie daarover: M.F.H. Hirsch Ballin and M. Galič, ‘Digital Investigation Powers and Privacy. Recent ECtHR case law and implications for the modernization of the Code of Criminal Procedure’, *Boom Strafblad* 2021, 4, 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*, Nijmegen: Radboud University Press 2022 (hierna: Fedorova e.a. 2022) en B.W. Schermer & M. Galič, ‘Biedt de Wet politiegegevens een stelsel van ‘end-to-end’ privacywaarborgen?’, *Nederlands Tijdschrift voor Strafrecht* 2022, nr. 3, p. 167-177 (hierna: Schermer & Galič 2022).

and Case Study for Investigating Organized Crime and Serving the Public Interest' uit 2021 geven (voormalig) medewerkers van het Nederlandse politieteam een toelichting op het concept van datagedreven opsporing.[12]

Kortgezegd bestaat het concept voor datagedreven opsporing uit de volgende vier stappen.

1. *Verzamelen*: het verzamelen van de gegevens (ook wel 'data' genoemd). Niet alleen uit voorgaande operaties, maar ook door het verzamelen van nieuwe 'strategische datasets';
2. *Opslaan*: het eenduidig bewerken en opslaan van de gegevens en deze vervolgens bundelen tot stukjes informatie die relevant zijn voor de opsporing;
3. *Analyseren*: het koppelen van informatiepunten met kennis door middel van uiteenlopende 'tools' (software). Hierbij worden gegevens verrijkt met reeds bekende informatie.
4. *Interveniëren*: hier wordt overgaan tot daadwerkelijke interventie(s) op basis van de geanalyseerde informatie ('intelligence').[13] Een interventie kan zich zowel richten op de dader, als op het slachtoffer, als op de criminele infrastructuur.[14]

Bovenstaande manier van werken – en de betrouwbaarheid daarvan – kwam naar ons weten voor het eerst in de 'Naoufal F.'-zaak aan de orde.[15] In de strafzaak wordt een deel van de berichten gebruikt die eerder waren verzameld van cryptotelefoon-provider 'Ennetcom'. De gegevens zijn vervolgens met het innovatieve systeem 'Hansken' van het Nederlands Forensisch Instituut (NFI) verwerkt en geanalyseerd.[16] De werking van het Hansken-systeem als aan de orde in de Naoufal F.-zaak vormt een goed voorbeeld van datagedreven opsporing. Wij lichten dat hierna toe.

1. *Verzamelen*

In 2016, had het Nederlandse *Team High Tech Crime* in totaal 3,7 miljoen berichten via een rechtshulpverzoek verzameld en veiliggesteld op een server bij het bedrijf Ennetcom in Canada.[17] Het bedrijf leverde cryptotelefoons en diensten op het gebied van versleutelde communicatie. Klanten konden met BlackBerry-telefoons, voorzien van specifieke software,

12 E. van de Sandt, A. van Bunningen, J. van Lenthe & J. Fokker, 'Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest', paper presented at the Third INTERPOL-UNICRI Global Meeting on AI for Law Enforcement on 25 November 2020, REPHRAIN (versie maart 2021) (hierna: Van de Sandt e.a. 2021).

13 De begrippen 'data', informatie en intelligence kunnen als volgt worden uitgelegd. Data zijn de door mensen vastgelegde feiten en gegevens. Informatie wordt begrepen als het product van het plaatsen van data in een context en de interpretatie ervan. Intelligence gaat nog een stap verder: door de combinatie van informatie met kennis die al beschikbaar is, wordt de informatie 'actiegericht' gemaakt. Zie W. Huisman, 'Slimmer strafrecht? Het MIT en de data gedreven opsporing', *DD* 2022/14.

14 Van de Sandt e.a. 2021, p. 2. Zie ook C.A.J. van Eeden, J.J. van Berkel, C.C. Lankhaar & C.J. de Poot, 'Opsporen, vervolgen en tegenhouden van cybercriminaliteit', WODC, Cahiers 2021-23, p. 47 (hierna: Van Eeden e.a. 2021).

15 Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504. Zie ook J. Henseler, 'Het inzagerecht en de groeiende omvang van digitaal bewijs', Expertise en Recht 2020, nr. 6, p. 215-217 en Egberts 2022.

16 Zie 'Uitspraak gebruik Ennetcom-data: Hansken doorstaat juridische toets', 20 april 2018, *forensischinstituut.nl*. Zie ook informatieblad 'Forensische waarborgen in Hansken' (2021) op Hansken.nl over de werking van het systeem en R.B. Van Baar, H.M.A. van Beek & E.J. van Eijk, 'Digital Forensics as a Service: A game changer', *Digital Investigation* 2014, S54–S56, H.M.A. van Beek, e.a., 'Digital forensics as a service: Game on', *Digital Investigation* 2015, p. 20-28 en H.M.A. van Beek, e.a., 'Digital forensics as a service: Stepping up the game', *Digital Investigation* 2020, p. 1-13.

17 T. Kreling, 'Justitie heeft toegang tot 3,6 miljoen versleutelde berichten van criminelen', *De Volkskrant*, 9 maart 2017. De Ennetcom-operatie is ook uitvoerig beschreven in B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3 (hierna: Schermer & Oerlemans 2020). Zie over de feiten omtrent de verzameling ook HR 8 maart 2022, ECLI:NL:PHR:2022:219, concl. A-G Harteveld, 2.5-2.8.

versleutelde tekstberichten versturen.[18] De Hoge Raad achtte onlangs de vergaring van deze gegevens en het gebruik ervan als bewijs rechtmatig.[19]

2. *Opslaan*

De veiliggestelde gegevens van cryptotelefoon provider Ennetcom zijn vervolgens ingeladen in het Hansken-systeem van het NFI. In deze tweede fase van 'opslaan' extraheert Hansken de gegevens van de servers voor de nadere verwerking. In het extractieproces stuurt Hansken de gegevens herhalend naar tientallen forensische tools om zoveel mogelijk sporen uit de bewijsbestanden te halen.

Enkele voorbeelden zijn tools die e-mails en contactpersonen uit e-maildatabases lezen en tools die tekst uit afbeeldingen kunnen halen.[20] De verwerking bestaat ook uit het toevoegen van metadata (tijdstip en datum van bericht en de naam van de afzender bijvoorbeeld) en het creëren en vergroten van een zoekwoordenindex (met woorden die bijvoorbeeld voorkomen in een bericht). De onderliggende bestanden met data ('ruwe data') worden ongewijzigd opgeslagen en zijn ook raadpleegbaar. Het Hansken-systeem is inmiddels gebruikt in meer dan 1000 strafzaken in Nederland, waaronder dus de Ennetcom-zaken.[21]

3. *Analyseren*

Voor de analyse van de gegevens in Hansken worden tientallen forensische tools gebruikt. Hansken moet daarom worden gezien als een krachtig 'platform' voor digitaal forensisch onderzoek. Hansken maakt daarbij gebruik van 'big data': door het gebruik van grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden data geanalyseerd, waarbij naar gegevens en correlaties wordt gezocht die kennis kunnen opleveren op basis waarvan beslissingen kunnen worden genomen. Hierbij worden grote hoeveelheden data geanalyseerd om aan de hand daarvan kennis te vergaren over bijvoorbeeld een verdachte.[22]

Met de tools is het bijvoorbeeld mogelijk een tijdlijn te maken en netwerken van apparaten in kaart te brengen die zijn gekoppeld aan personen. Het is ook mogelijk gegevens te doorzoeken op bepaalde kenmerken zoals een 'nickname' van een gebruiker van een toestel of op basis van zoekwoorden. Rechercheurs kunnen ook door middel van filters een dataset samenstellen en dan daarin verder zoeken. Bij Ennetcom zijn de gegevens ook gefilterd met behulp van bepaalde zoektermen die te maken hadden met – onder andere – drugstransporten.[23] Daarmee wordt een subset van gegevens gecreëerd waarin rechercheurs verder mogen zoeken. Bij Ennetcom werd voor het creëren van een subset voor andere

18 De oprichter en tevens leverancier van Ennetcom-telefoons is veroordeeld voor (gewoonte)witwassen, deelname aan een criminele organisatie, valsheid in geschrifte en verboden wapenbezit. Zie Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085, *TBS&H* 2022, m.nt. J.J. Oerlemans.

19 HR 28 juni 2022, ECLI:NL:HR:2022:900, r.o. 3.5.1-3.6.6.

20 Zie de Gegevensbeschermingseffectboordeling (PIA), zaakonderzoek uitgevoerd met Hansken Variant 1A "inzet als forensisch onderzoeker", 19 september 2019, Den Haag: ministerie van Justitie en Veiligheid – Nederlands Forensisch Instituut (NFI), p. 32.

21 'Hansken Product Vision', mei 2022, p. 6.

22 Zie de Gegevensbeschermingseffectboordeling (PIA), zaakonderzoek uitgevoerd met Hansken Variant 1A "inzet als forensisch onderzoeker", 19 september 2019, Den Haag: ministerie van Justitie en Veiligheid – Nederlands Forensisch Instituut (NFI), p. 12.

23 Laurens Verhagen, 'Met deze eigen zoekmachine spit de politie schatten aan digitaal bewijs door', *De Volkskrant*, 12 oktober 2018.

strafrechtelijke onderzoeken van tevoren toestemming van de rechter-commissaris gezocht en verkregen.[24]

In de zaak tegen Naoufal F. werd er aanleiding gezien de berichten in de Ennetcom-dataset te doorzoeken, omdat in een andere (moord)zaak cryptotelefoons in beslag waren genomen waarmee werd gecommuniceerd met het toestel van Naoufal F. Een dataset van gegevens van de Ennetcom-servers is vervolgens gecreëerd en onderzocht aan de hand van:
1. de e-mailadressen, IMEI-nummers en PIN-nummers die aan de verdachten in het onderzoek Tandem zijn gerelateerd;
2. e-mailaccounts die voorkomen in de berichten van e-mailadressen en de contactpersonen van telefoontoestellen; en
3. (bij)namen (nicknames) van de verdachten in het onderzoek 'Tandem'.

4. *Interveniëren*

De verwerking van gegevens ten behoeve van de opsporing moet worden gezien als één van de interventiemogelijkheden binnen het concept van datagedreven opsporing. In de Naoufal F.-zaak droegen de gegevens bij aan het bewijs voor het medeplegen van moord. De rechtbank was in de zaak overigens overtuigd van de betrouwbaarheid van het bewijs zoals dat voortkwam uit de toepassing van het Hansken-systeem. Daarbij speelde mee dat de verdediging in de gelegenheid werd gesteld twee bezoeken te brengen aan het NFI met een eigen, niet-geregistreerde, deskundige. Zij hebben zelf onderzoek kunnen doen in het systeem en de verdediging heeft in totaal 110 schriftelijke vragen aan het NFI kunnen stellen. Nadat die vragen zijn beantwoord, heeft de rechter-commissaris de deskundige nog gehoord, waarbij de verdediging eveneens in de gelegenheid is gesteld om vragen te stellen.[25]

Het bovenstaande voorbeeld van Ennetcom en het gebruik van een deel van die gegevens voor een moordzaak zijn illustratief voor het concept van datagedreven opsporing. Het Team High Tech Crime van de Nederlandse politie maakt al langer gebruik van de strategie. Het Team High Tech Crime heeft reeds jarenlange ervaring in het veiligstellen van grote datasets en verdere gebruik van de gegevens ten behoeve van opsporing en verstoring van cybercriminaliteit.[26]

Het WODC-rapport 'Opsporen, vervolgen en tegenhouden van cybercriminaliteit' maakt bovendien duidelijk dat gegevens ook verzameld en verwerkt worden voor handhavingsdoeleinden, naast opsporing.[27] Binnen de praktijk van de bestrijding van cybercriminaliteit is dit bijvoorbeeld zichtbaar in de toepassing van het instrument van 'knock and talk acties'. Een knock and talk actie betreft een waarschuwingsgesprek waarbij de politie in gesprek gaat met (potentiële) verdachten over de strafbaarheid van hun gedrag. Het doel van het waarschuwingsgesprek is afschrikken door het signaal af te geven dat de politie toezicht houdt en dat verdachten minder anoniem zijn dan ze denken. In het geval van jongeren

24 Van Beek 2020, p. 1. Zie ook Menno van Dongen, 'Gaat justitie te ver met de miljoenen onderschepte berichten van criminelen? De Hoge Raad beslist het vandaag', *De Volkskrant,* 28 juni 2022.

25 Zie ook Schermer & Oerlemans 2020.

26 De Robert M.-zaak (Rb. Den Haag 24 januari 2012, ECLI:NL:RBSGR:2012:BV1693) vormt een goed voorbeeld. De politie heeft in dat onderzoek - alweer meer dan 10 jaar geleden - 8 Terabyte (8000 Gigabyte) aan materiaal in beslag genomen, met 58.000 tekstpagina's, foto's, video's, Skypecommunicatie en webmail. Door de gegevensvergaring in dit onderzoek – met de naam 'Holitna' – zijn in totaal 508 kinderpornozaken in beeld gekomen en 33 arrestaties verricht ('Veel complex materiaal in onderzoek zedenzaak', 30 mei 2012, *Nu.nl).*

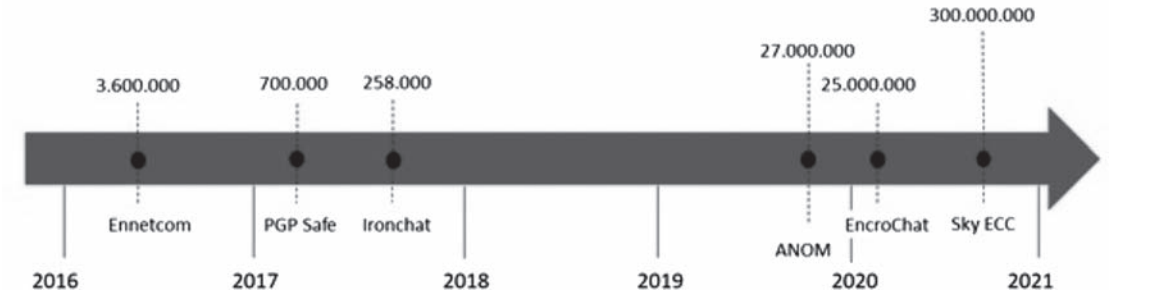
27 Zie ook Van Eeden e.a. 2021, p. 50.

wordt ook in gesprek gegaan met de ouders, die naar aanleiding van een dergelijk gesprek bijvoorbeeld meer toezicht op hun kind kunnen houden.[28]

Door het aangehaalde WODC-onderzoek en het rapport waarin het concept van datagedreven onderzoek uiteen wordt gezet, is duidelijk dat bijzondere opsporingsbevoegdheden óók (naast het opsporingsdoel) voor strategische redenen worden ingezet, zoals het zicht krijgen op een bepaald criminaliteitsfenomeen en voor kennis ten behoeve van volgende opsporingsonderzoeken.[29] In dat kader wordt opgemerkt dat:

> "De politie zou graag los van concrete onderzoeken samen met andere partijen activiteiten van (internationale) criminele groeperingen, facilitators en andere daders willen blijven volgen om daar een informatiepositie over op te bouwen. Om dit te bewerkstelligen streeft THTC naar een datagedreven manier van werken. Zo kan gekeken worden of er verbanden kunnen worden gelegd tussen data uit verschillende opsporingsonderzoeken om bijvoorbeeld na te gaan of er overeenkomsten zijn in modus operandi of gebruikte malware."[30]

Wij wijzen erop dat na Ennetcom diverse andere cryptotelefoonoperaties door of met betrokkenheid van de Nederlandse politie zijn uitgevoerd. Ook door deze operaties zijn gegevens veiliggesteld van de providers van cryptotelefoons en de versleutelde communicatie van 'Ennetcom', 'PGP Safe', 'IronChat', 'ANOM', 'EncroChat' en 'Sky ECC'. Daarbij zijn telkens grote hoeveelheden gegevens verzameld. Een overzicht van de cryptotelefoonoperaties met een tijdlijn is in Figuur 1 zichtbaar gemaakt.



Figuur 1: Overzicht van cryptotelefoonoperaties.[31]

Bij EncroChat en Sky ECC zijn tientallen tot honderden miljoenen gegevens veiliggesteld van servers bij een hosting provider in Frankrijk.[32] Inmiddels zijn er al honderden uitspraken gepubliceerd waarin gegevens uit cryptotelefoonoperaties een rol speelden in het bewijs ten behoeve van de veroordeling van verdachten.[33]

Kortom: het concept van datagedreven opsporing en de cryptotelefoonoperaties zijn geen 'high tech' operaties in de marge van de opsporing, maar spelen een wezenlijke rol in de strafrechtspleging en leiden tot een fundamentele verschuiving in de werkwijze van de

28 E. van 't Zand, S. Matthijsse, T. Fischer & W. van der Wagen, 'Interventies voor cyberdaders', p. 287 in: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (red.), *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk*, Den Haag: Boom criminologie 2020.
29 Van Eeden e.a. 2021, p. 58 en Van de Sandt e.a. 2021, p. 13.
30 Van Eeden e.a. 2021, p. 40.
31 Bron: J.J. Oerlemans, 'Overzicht cryptophone-operaties', *jjoerlemans.com*, 14 november 2022.
32 De Encrochat-operatie ('26Lemont') wordt uitvoering beschreven in Schermer & Oerlemans 2022.
33 Het aantal "honderden strafzaken" is gebaseerd op een zoekslag op rechtspraak.nl met de woorden 'EncroChat', 'Sky ECC', 'ANOM', 'IronChat' of 'PGP Safe', gefilterd op uitspraken van strafrechtelijke instanties.

opsporing. Datagedreven opsporing verdient aldus de volle aandacht van de strafrechtswetenschap.

3. De juridische grondslag voor datagedreven opsporing

De wetgever heeft in het Wetboek van Strafvordering alleen bevoegdheden tot verzameling van gegevens willen regelen. Bevoegdheden voor de verwerking en analyse van de verzamelde gegevens zijn geregeld in de Wet politiegegevens (Wpg) en in de Wet justitiële en strafvorderlijke gegevens (Wjsg).[34] Ook in de voorstellen voor het nieuwe Wetboek van Strafvordering wordt (vooralsnog) vastgehouden aan deze (harde) knip in de wettelijke regeling tussen bevoegdheden tot vergaring van data en bevoegdheden tot verwerking van de vergaarde data.[35] Noch het Wetboek van Strafvordering, noch de Wet politiegegevens (Wpg) geeft bevoegdheden voor het verzamelen van gegevens aan de politie voor intelligence-doeleinden. Wel kunnen gegevens die zijn vergaard in het kader van de politietaak ex artikel 3 Politiewet 2012 (die breder is dan alleen de opsporing) worden gebruikt voor intelligence-doeleinden. Deze 'intelligence-taak' van de politie wordt niet genormeerd in het Wetboek van Strafvordering, maar heeft haar wettelijke basis in de Wpg.[36] Het in paragraaf 2 beschreven concept van datagedreven opsporing wordt in de praktijk dan ook gebaseerd op de Wpg.[37]

De uitvoering van de intelligence-activiteiten van de politie wordt vooral gestoeld op artikel 10 en artikel 11 Wpg.[38] Op grond van artikel 10 Wpg kunnen politiegegevens gericht worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij – kort gezegd – (categorieën van) ernstige misdrijven. De wet biedt daarnaast de mogelijkheid in artikel 11 Wpg om de gegevens uit opsporingsonderzoeken en gegevens die worden verwerkt op grond van artikel 8, 9 of 10 Wpg geautomatiseerd te vergelijken en in combinatie te doorzoeken.[39]

Gelet op het doelbindingsprincipe mogen gegevens slechts worden verwerkt ten behoeve van het doel waarvoor zij zijn verzameld. Echter, op grond van artikel 11 lid 4 Wpg mag het 'bevoegd gezag', dat wil zeggen de officier van justitie, goedkeuring geven voor de verwerking van gegevens voor andere doeleinden.[40] Dit betekent dat gegevens tussen onderzoeken kunnen worden gedeeld, maar ook voor andere taken mogen worden gebruikt.[41] Daarbij moet een 'zorgvuldige afweging' worden gemaakt tussen het belang dat met de raadpleging van andere onderzoeksgegevens is gediend en het belang van de personen van wie de gegevens kunnen worden betrokken in dit onderzoek. De wetgever noemt hierbij dat daarbij 'onder meer de beginselen van proportionaliteit en subsidiariteit' in acht moeten worden genomen.[42]

34 Vgl. Fedorova e.a. 2022, p. 29.
35 Fedorova e.a. 2022 en Schermer 2022.
36 B.W. Schermer, 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen strafvordering en de Wet politiegegevens', *TBS&H* 2017, afl. 4, p. 209 (hierna: Schermer 2017). Zie ook M.J. Dubelaar, M.I. Fedorova & R.M. te Molder, 'De vergaring en het gebruik van digitale gegevens in een strafvorderlijke context', in P.T.J. Wolters, *Digitalisering en conflictoplossing,* Deventer: Wolters Kluwer 2021, p. 59.
37 Van Eeden e.a. 2021, p. 43.
38 Schermer 2017, p. 209.
39 Idem, p. 211. Zie ook Fedorova e.a. 2022, p. 23-24.
40 Zie ook Schermer & Galič 2022, p. 170.
41 Zie ook Van Eeden e.a. 2021, p. 86.
42 *Kamerstukken II* 2005/06, 30327, nr. 3, p. 51.

Gegevens die zijn verkregen na de toepassing van bepaalde bijzondere opsporingsbevoegdheden, waaronder het opnemen van vertrouwelijke communicatie of telecommunicatie en het vorderen van gegevens, kunnen door de officier van justitie op grond van artikel 126dd Sv worden verstrekt voor gebruik in andere opsporingsonderzoeken of voor verwerking op grond van artikel 10 Wpg.[43] In de memorie van toelichting wordt deze praktijk als volgt beschreven:

> "Gegevens die in het ene onderzoek zijn verkregen door toepassing van ingrijpende bevoegdheden, bijvoorbeeld de inbeslagneming van een boekhouding, kunnen op deze wijze beschikbaar komen voor een ander onderzoek dat op zichzelf geen aanleiding had kunnen geven tot de inbeslagneming. Hierbij moet ook worden bedacht dat de gegevens, die in het kader van de artikelen 9 en 10 worden verwerkt niet altijd op juistheid en volledigheid zijn of kunnen worden getoetst. Het kan hier ook gaan om zogenaamde "bulkgegevens", gegevens die zijn verkregen door middel van telefoontaps en de inbeslagneming van computergegevens, waarbij nog niet is geselecteerd welke van die gegevens relevant zijn voor het onderzoek. Onder deze bulkgegevens kunnen zich ook gegevens van niet-verdachte burgers bevinden."[44]

Uit de jurisprudentie blijkt dat de 126dd-bevoegdheid veelvuldig wordt toegepast in (datagedreven) opsporingsonderzoeken die zijn voortgekomen uit de cryptophone-operaties.[45] Overigens moet daarbij worden opgemerkt dat in de zaken naar aanleiding van de Encrochat-operatie niet alleen de officier van justitie het bevel op grond van artikel 126dd Sv heeft gegeven voor de verdere verwerking in andere onderzoeken, maar dit ook is gemachtigd door de rechter-commissaris. In deze zaken heeft de rechter-commissaris dus óók toestemming gegeven voor het creëren van een subset van de gegevens ten behoeve van andere onderzoeken, terwijl een dergelijke machtiging door de rechter-commissaris op grond van de wet niet is vereist.[46]

Ook in het arrest van de Hoge Raad van 28 juni 2022 (inzake Ennetcom) was een dergelijke machtiging van de rechter-commissaris aan de orde. Het ging er in die zaak om dat de Canadese autoriteiten bij de overdracht als voorwaarde hadden gesteld dat een voorafgaande rechterlijke machtiging nodig was voor het gebruik van (een deel van) de gegevens ten behoeve van een andere strafzaak. De Hoge Raad achtte deze gang van zaken (zonder specifieke wettelijke grondslag), tegen de achtergrond van de gestelde voorwaarden bij de rechtshulp rechtmatig. Dat geldt ook voor het verlenen van de opdracht in één van de machtigingen van de rechter-commissaris om de voor het onderzoek relevante gegevens te selecteren.[47]

---

43 Idem, p. 210. Schermer (2017) merkt op dat deze gegevens ook verstrekt kunnen worden ten behoeve van de intelligence-taak van de politie op grond van art. 10 lid 1 onder b Wpg jo. art. 126dd lid 1 onder b Sv.

44 *Kamerstukken II* 2005/06, 30327, nr. 3, p. 51.

45 Zie bijvoorbeeld Rb. Amsterdam 15 februari 2022, ECLI:NL:RBAMS:2022:568, Rb. Oost-Brabant 19 mei 2022, ECLI:NL:RBOBR:2022:1993 en Rb. Amsterdam 26 november 2021, ECLI:NL:RBAMS:2021:6866.

46 Zie bijvoorbeeld Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584 en Egberts 2022, p. 123. Zie ook Rb. Limburg 14 maart 2022, ECLI:NL:RBLIM:2022:1992, met het citaat uit een proces-verbaal: "**Toestemming rechter-commissaris voor uitbreiding aanvullend onderzoek naar Sky-accounts**". *De rechter-commissaris heeft op 2 april 2021 uitbreiding* aanvullende toestemming *verleend om de voor onderzoek Graniet relevante gegevens vanuit Argus te gebruiken. Het OM Argus had eerder toestemming gebruik gegevens voor een ander doel afgegeven (art. 126dd, lid 1 Wetboek van Strafvordering). De beslissing van de rechter commissaris behelst onderstaande Sky-accounts en de daarbij behorende kaders [..]*".

47 HR 28 juni 2022, ECLI:NL:HR:2022:900, r.o. 3.6.3-3.6.4.

4. Verbreding van doelstellingen van strafvorderlijk optreden

Datagedreven opsporing volgens de hiervoor beschreven praktijk heeft een ander karakter dan de 'reguliere' opsporing, omdat het doel (of de doelen) ervan breder is (zijn) dan het 'traditionele' doel van bewijsvergaring in onderzoeken in verband met (gepleegde of te plegen) strafbare feiten met het oog op het nemen van een strafvorderlijke beslissing in relatie tot verdachten (vgl. artikel 132a Sv). Datagedreven opsporing richt zich op het ontdekken van (nieuwe) strafbare feiten en met het oog op interventies niet alleen ten aanzien van verdachten, maar ook ten behoeve van het slachtoffer of ter verstoring van de criminele infrastructuur. Het ontdekken van nieuwe strafbare feiten is bovendien van een andere aard dan voorzien in de wettelijke grondslagen van het verkennend onderzoek ex artikel 126gg Sv en de verwerking van politiegegevens ter uitvoering van de politietaak op grond van artikel 10 Wpg jo. artikel 3 Politiewet 2012. Dit lichten wij in deze paragraaf nader toe.

Bij datagedreven opsporing gaat het om het opwerken van bestaande informatie naar 'intelligence'; oftewel het gaat om het proces van bij elkaar brengen en analyseren van hetgeen al bekend is, naar het opwerken naar nieuwe, ge(re)construeerde feiten ten behoeve van andere, nieuwe, onderzoeken.[48] Anders dan bij de 'reguliere' opsporing, heeft de datagedreven opsporing dus een duidelijke nevendoelstelling die kan worden getypeerd als een intelligence-functie.[49] Door in een concreet onderzoek de scope van het onderzoek zo breed mogelijk te houden, verkregen gegevens te combineren met andere politiegegevens en te analyseren met software ('tools') voor gegevensverwerking worden nieuwe inzichten verworven en ontstaat zicht op nog niet eerder ontdekte strafbare feiten. Het verkrijgen van deze intelligence kan lastig worden begrepen als bijvangst van opsporingsonderzoeken, omdat het in feite de motor is (een goudmijn aan bewijs) voor nieuw strafrechtelijk onderzoek.

Deze intelligencefunctie heeft daarom ook een belangrijke zelfstandige rol naast het doel van bewijsverzameling. Hier gebeurt dus iets anders dan was voorzien door de wetgever bij de strafvorderlijke normering van de opsporing. In de reguliere opsporing en de daarvoor ontworpen normering van Wetboek van Strafvordering gaat het immers om de bescherming van de rechten van de subjecten die voorwerp van onderzoek zijn, de verdachte of andere subjecten in het kader van het onderzoek naar of de zoektocht naar de verdachte, in verband met het voorliggende onderzoek naar een verdenking (of aanwijzingen) van een concreet strafbaar feit. Dat geldt ook voor het onderzoek op basis van een verdenking van voorbereidingshandelingen of deelneming aan een criminele organisatie of in het kader van het proactieve onderzoek naar het beramen of plegen van misdrijven in georganiseerd verband[50] of naar aanwijzingen van een terroristisch misdrijf.[51] Ook in die opsporingsonderzoeken wordt bewijs vergaard mede met het oog op het voorkomen van andere (ernstigere) misdrijven. Dat is echter wat anders dan de gerichtheid op het vergaren van gegevens, zodat die gegevens kunnen worden gecombineerd en geanalyseerd met andere gegevens en uit die analyses verdenkingen of aanwijzingen voortvloeien voor nieuwe

48 Vgl.: Hirsch Ballin 2022-1.

49 Zie ook B.W. Schermer, 'De gespannen relatie tussen privacy en cybercrime', inaugurele rede ter aanvaarding van het ambt van Hoogleraar Privacy en Cybercrime, Universiteit Leiden 2022 (hierna: Schermer 2022).

50 Door toepassing van de bijzondere opsporingsbevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband (Titel V).

51 Door toepassing van de bijzondere opsporingsbevoegdheden bevoegdheden tot opsporing van terroristische misdrijven (Titel VB).

opsporingsonderzoeken. De consequenties van inzet van opsporingsbevoegdheden in een concreet onderzoek, gaan in dat geval veel verder en raken aan een veel grotere groep van subjecten dan de verdachte(n) in het concrete onderzoek.

Die verbreding van de doelstelling van de opsporing bij de datagedreven opsporing, in het bijzonder wat betreft de mogelijkheden om nieuwe gegevens te ontdekken of te (re)construeren ten behoeve van nieuwe opsporingsonderzoeken, komt nu naar voren bij de zaken die voortvloeien uit de cryptotelefoonoperaties. De enorme hoeveelheid gegevens waarover door hacks van cryptotelefoons de beschikking wordt verkregen in een concrete zaak, zijn door de geavanceerde analyse ervan een ongekende bron om nieuwe strafbare feiten te ontdekken en politie-intelligence te genereren.

Vooral in onderzoeken die cybercriminaliteit betreffen is zichtbaar dat de inzet van opsporing zich uitdrukkelijker richt op andere interventies dan alleen de traditionele van bewijsvergaring ten behoeve van vervolging en berechting van verdachten. Dat sluit aan bij de gedachte dat cybercriminaliteit ook – of misschien zelfs *beter* – wordt bestreden door de criminele infrastructuur uit te schakelen waardoor een delict als computervredebreuk kan worden stopgezet of kwaadaardige software (malware) niet meer kan worden geactiveerd op een computer.[52] Dat uitschakelen gebeurt voorts niet (alleen) door verdachten te vervolgen en berechten, maar ook door criminaliteit te 'verstoren', bijvoorbeeld door het onderuithalen van het (cyber)criminele verdienmodel, de activiteiten van een tussenpersoon bij witwassen stop te zetten of het vertrouwen op een digitale drugsmarkt onderuit te halen.[53] Hierbij past ook de politiestrategie die zich op de aanpak van *facilitators* richt, oftewel personen of organisaties die criminelen of criminele organisaties (digitaal) ondersteunen of faciliteren.[54] Het gaat dus telkens om een combinatie van meer traditionele opsporing en vervolging, zoals ook de opsporing en vervolging voor voorbereidingshandelingen of deelname aan een criminele organisatie, en van interventies die *sec* zijn gericht op het tegenhouden of stoppen van de criminele activiteiten.

Hoofddoelstelling van ons strafprocesrecht – en daaraan wordt in het nieuwe Wetboek van Strafvordering vastgehouden[55] – is het bevorderen dat de strafwet wordt toegepast op de werkelijk schuldige, en te voorkomen dat de onschuldige wordt veroordeeld of zelfs wordt vervolgd.[56] Dit heeft te betekenen dat in de regels die ons strafprocesrecht vor-

52 Ook een van de ratio's van de introductie van de hackbevoegdheid in artikel 126nba Sv. *Kamerstukken II* 2015/16, 34372, 3, p. 29.

53 Van Eeden e.a. 2021, p. 64: "*Uit dit onderzoek komt naar voren dat opsporing en tegenhouden van criminele processen hand in hand gaan, omdat dat in de optiek van de geïnterviewde de meest effectieve manier is om cybercriminaliteit aan te pakken. Hierbij werd ook verwezen naar de aanpak bij ondermijning, waar de aanpak heel specifiek is gericht op het criminele verdienmodel.*"

54 Zie 'Ontsleutelde berichtgeving crypto-gsm's cruciaal in zaak vergismoord', *OM.nl*, 11 december 2017. De verdachte *facilitator* van versleutelde communicatie is overigens vrijgesproken van het delict deelname aan criminele organisatie (Rb. Rotterdam 20 januari 2022, ECLI:NL:RBROT:2022:363). Zie ook 'Klap voor communicatie criminelen: DoubleVPN uit de lucht', *OM.nl*, 30 juni 2021 en het 'Internet Organised Crime Threat Assessment' rapport van Europol uit 2021, waarin Europol dat Europese opsporingsdiensten zich steeds meer richten op diensten die cybercriminelen zoveel mogelijk beschermen van opsporingsdiensten. Recente voorbeelden zijn de 'take downs' van 'ANOM', 'Sky ECC', 'EncroChat', 'VPN-diensten' en 'cryptocurrency mixers'. Het zijn volgens Europol voorbeelden van 'grijze infrastructuur' waar cybercriminelen gebruik van maken.

55 Conceptmemorie van toelichting nieuw Wetboek van Strafvordering (ambtelijke versie juli 2020), p. 10-12.

56 *Kamerstukken II* 1913/14, 286, nr. 3, p. 55 en G.J.M. Corstens, *Het Nederlands strafprocesrecht,* bewerkt door M.J. Borgers en T. Kooijmans, Deventer: Wolters Kluwer 2021, p. 8.

men de materiële waarheidsvinding centraal staat, in een proces dat is ingericht op een wijze die uitdrukking geeft aan de onschuldpresumptie. De strafvorderlijke normering van bevoegdheden neergelegd in ons Wetboek van Strafvordering is dus eveneens op die hoofddoelstelling georiënteerd. In de normering van de opsporingsbevoegdheden komt dat tot uitdrukking doordat de aanleiding voor inzet ervan dient te worden gevonden in feiten en omstandigheden die wijzen op (gepleegde of te plegen) strafbare feiten en dat de bevoegdheid alleen wordt ingezet voor het doel waarvoor het is gegeven en voor zover dat in het belang van het onderzoek is.[57] Ook in het conceptwetsvoorstel voor het nieuwe Wetboek van Strafvordering wordt aan dit uitgangspunt voor de inzet van bevoegdheden vastgehouden. De beginselen van doelbinding en noodzakelijkheid worden daarbij ook als algemene beginselen voor de bevoegdheidsuitoefening in de opsporing neergelegd in het beoogde artikel 2.1.2.[58] De uitgangspunten en daarmee de oriëntatie op de bewijsvergaring voor vervolging en berechting voor opsporingsbevoegdheden die een grondslag hebben in het Wetboek van Strafvordering gelden aldus in het nieuwe Wetboek onverkort. Dat neemt niet weg dat het opsporingsbegrip inmiddels een bredere reikwijdte heeft gekregen. Het begrip beslaat tegenwoordig een breed spectrum van onderzoek 'in verband met strafbare feiten', zonder dat daarbij is vereist dat sprake is van een redelijk vermoeden van schuld of zelfs een aanwijzing van een strafbaar feit.[59] Als gevolg daarvan komt het opsporingsbegrip tegemoet aan het bredere karakter van strafvorderlijke reacties, dat in de praktijk al lang niet meer is beperkt tot bewijsvergaring voor vervolging en berechting van verdachten.

Deze hoofddoelstelling van ons strafprocesrecht is dus bepalend voor de wijze waarop bevoegdheden worden genormeerd. Dat betekent tegelijkertijd niet dat die hoofddoelstelling in de weg staat aan andersoortige reacties dan de traditionele van oplegging van een strafrechtelijke sanctie door de rechter aan de daadwerkelijk schuldige. De oplegging van de strafbeschikking door het openbaar ministerie is een voorbeeld van zo'n andersoortige reactie die wordt geregeld in het strafprocesrecht. Ook het opsporingsbegrip komt een bredere betekenis toe dan alleen het onderzoek ten behoeve van de berechting van de verdachte. De term van strafvorderlijke beslissingen (in artikel 132a Sv) wordt breed uitgelegd en omvat ook andersoortige strafvorderlijke reacties. Voorts geeft het opsporingsbegrip de ruimte voor het nastreven van andersoortige doelen en reacties (zoals hiervoor beschreven in relatie tot de cybercriminaliteit). Niettemin geldt ten aanzien van opsporingsbevoegdheden genormeerd in het Wetboek van Strafvordering nog altijd het doelbindingsprincipe, op grond waarvan de inzet dient te worden beperkt tot het traditionele doel van strafvordering. Dat staat tegelijkertijd op zichzelf dus niet aan andersoortige reacties of doelen in de weg.[60]

---

57 Vgl. de memorie van toelichting van de Wet bijzondere opsporingsbevoegdheden: *"De bevoegdheden strekken ertoe onderzoek te kunnen doen, met als doel de opheldering en afdoening van strafbare feiten. Dit doel rechtvaardigt een plaats van deze bevoegdheden in het Wetboek van Strafvordering.*" (*Kamerstukken II* 1996/97,25403, nr. 3, p. 3 en vgl. p. 6-7, 99-100). Zie ook: M.F.H. Hirsch Ballin, *Anticipative Criminal Investigation. Theory and Counterterrorism Practice in the Netherlands and the United States* (diss. Utrecht), T.M.C. Asser press/Springer 2012, p. 121-123.

58 Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (ambtelijke versie juli 2020), boek 2.

59 Zie L. Stevens e.a., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling', *TBS&H* 2021, nr. 4, p. 241-242 (hierna Stevens e.a. 2021).

60 Het gaat het bestek van deze bijdrage te buiten om de reikwijdte van het opsporingsbegrip en de betekenis van het strafvorderlijke doelbindingsbeginsel volledig uit te werken. Wij verwijzen in dat verband naar: M.F.H. Hirsch Ballin, *Responsief strafprocesrecht in een netwerk van rechtsbetrekkingen*, preadvies CJV 2022, p. 9-10 en 19-22 (hierna: Hirsch Ballin 2022-2).

Daarmee dringt zich de vraag op of het doelbindingsprincipe voor strafvorderlijke bevoegdheidsuitoefening eveneens breder zal moeten worden opgevat, zodat de bevoegdheidsuitoefening binnen de opsporing zich uitdrukkelijker kan gaan richten op doelstellingen die verder afliggen van de van oudsher gekozen oriëntatie in ons Wetboek van Stafvordering van strafvorderlijke bevoegdheidsuitoefening op onderzoek ten behoeve van de vervolging en berechting van de daadwerkelijk schuldigen en de bescherming van onschuldigen. Oftewel: betekent de ruimere reikwijdte van het opsporingsbegrip ook dat een ruimer spectrum van doelstellingen kan worden nagestreefd binnen die opsporing, die uitdrukkelijker *naast* het opsporingsdoel of zelfs *in de plaats komen* van de hoofddoelstelling van strafvorderlijke bevoegdheidsuitoefening? Het gaat er daarbij om dat niet langer nodig is dat andersoortige doelstellingen slechts naast de traditionele opsporing een plek mogen hebben, maar dat die andersoortige doelstellingen – het tegenhouden/stoppen van strafbare feiten en het versterken van de informatiepositie ten behoeve van het voorkomen van andere strafbare feiten – ook een zelfstandige doelstelling van de uitoefening van bevoegdheden in de opsporing kunnen zijn. Wij beantwoorden die vraag positief, maar menen dat dit tegelijkertijd implicaties heeft voor de normering van bevoegdheidsuitoefening bij het nastreven van die andere doelstellingen.

5. Het spanningsveld met strafvordering

In het verlengde van de verbreding van doelstellingen wordt het spanningsveld zichtbaar tussen bevoegdheidsuitoefening op grond van de algemene politietaak of op basis van bepalingen in de Wet Politiegegevens en op grond van de bepalingen in het Wetboek van Strafvordering, waar de grondslagen zijn neergelegd voor meer ingrijpende opsporingsbevoegdheden.

Dat spanningsveld is er in de eerste plaats, omdat moet worden afgevraagd of de bedoelde bepalingen uit de Politiewet 2012 en de Wpg uit privacyrechtelijk oogpunt – in het bijzonder het gegevensbeschermingsrecht – wel voldoende zijn toegesneden om als grondslag te kunnen dienen voor analyse van grote hoeveelheden data, van aard en omvang als aan de orde bij datagedreven opsporing.[61]

In de tweede plaats, en daarom is het ons in dit artikel te doen, is sprake van een spanningsveld met (de uitgangspunten van) strafvordering gelet op het nagestreefde doel van datagedreven opsporing. In dit verband wordt in het WODC-onderzoek over opsporing van cybercriminaliteit opgemerkt:

> "het niet uitsluitend inzetten op opsporen en vervolgen bij de aanpak van cybercriminaliteit betekent dat soms ook in juridisch opzicht een grijs gebied wordt opgezocht".[62]

Als het de inzet van in het Wetboek van Strafvordering geregelde opsporingsbevoegdheden betreft voor *alleen* de vergaring van informatie voor andere, nieuwe onderzoeken, is dit echter geen 'grijs gebied'. Als de strafvorderlijke opsporingsbevoegdheid daarmee niet wordt ingezet in het belang van het betreffende opsporingsonderzoek, moet dat in strijd

61 Zie daarover Stevens e.a. 2021, p. 235-237, Fedorova e.a. 2022, m.n. p. 161-164 en Schermer & Galič 2022.
62 Van Eeden e.a. 2021, p. 65.

worden geacht met de vereisten van de strafvorderlijke doelbinding en noodzakelijkheid.[63] Dat neemt niet weg dat bij de inzet van strafvorderlijke bevoegdheden ook relevante gegevens voor andere onderzoeken kunnen en mogen worden vergaard. Voorts kan de *scope* van sommige opsporingsbevoegdheden breder zijn, omdat het toepassingscriterium de inzet niet beperkt op basis van een concreet redelijk vermoeden van een strafbaar feit. Voorbeelden van dergelijke bevoegdheden zijn de bijzondere opsporingsbevoegdheden voor onderzoek naar terroristische misdrijven op grond van 'aanwijzingen van een terroristisch misdrijf' en het verkennend onderzoek ex artikel 126gg Sv.[64]

De beperking van doelbinding geldt niet voor bevoegdheden die weliswaar (ook) in het kader van de opsporing worden ingezet, maar een grondslag hebben buiten het Wetboek van Strafvordering. Ook daar geldt een doelbindingsprincipe – het is immers ook een fundamenteel beginsel in het gegevensbeschermingsrecht[65] – maar het doel wordt daar bepaald door de betreffende wet waarin de bevoegdheid normering vindt. Voor de verwerking en analyse van gegevens op grond van de Wpg geldt daarbij dat deze dienen plaats te vinden in het kader van de uitvoering van de politietaak en, bij meer ingrijpende verwerkingen, nader worden ingeperkt tot bijvoorbeeld onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval (art. 9 lid 1 Wpg).[66]

Zoals volgt uit de beschrijving in paragraaf 2 van het model van datagedreven onderzoek dat nieuwe opsporingsonderzoeken worden geïnitieerd, na en op basis van de verwerking en analyse van reeds vergaarde gegevens. Zoals toegelicht in paragraaf 3 zijn de bepalingen van de Wpg de grondslag voor deze verwerking en analyse.[67] De analyses op grond van de bepalingen van de Wpg hebben door de wijze waarop zij thans worden ingezet in de context van de datagedreven opsporing, veel meer een strafvorderlijk karakter gekregen (zij moeten geacht worden deel uit te maken van de opsporing in de zin van artikel 132a Sv en staan telkens in rechtstreeks verband met de uitoefening van strafvorderlijke opsporingsbevoegdheden),[68] terwijl de doelen ervan juist verder afstaan van in de in het Wetboek van Strafvordering genormeerde opsporingsbevoegdheden (gericht op de waarheidsvinding voor vervolging en berechting). Een scheiding in de normering van strafvorderlijke bevoegdheidsuitoefening en analyse en verwerking van politiegegevens op grond van het doel van de bevoegdheidsuitoefening is in die gevallen uit normatief oogpunt onwenselijk. Het gaat er immers om dat het recht integrale bescherming biedt in relatie tot de ingreep in de rechten van de burger – in het bijzonder

63 Zie: *Kamerstukken II* 1996/97, 25403, nr. 3, p. 3 en vgl. Memorie van toelichting bij het Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (ambtelijke versie juli 2020), p. 248-249. Zie ook Van Eeden e.a. 2021, p. 65: "*Desalniettemin kunnen de benodigde bevoegdheden niet enkel voor dat doel worden ingezet. Voor de inzet van opsporingsbevoegdheden ten behoeve van verstoring bestaat tot op heden geen wettelijke grondslag*".

64 Zie hierover uitvoerig: Hirsch Ballin 2012, m.n. p. 129-131 en 172-180.

65 Zie Fedorova e.a. 2022, p. 165-167.

66 En bij de bevoegdheid ex artikel 10 Wpg met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige misdrijven. Verder wordt ook het bestuursrechtelijk rechtshandhavend optreden door het doelbindingsbeginsel uitgewerkt in artikel 5:134 Awb: de toezichthouder maakt slechts gebruik van zijn bevoegdheden voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is.

67 Van Eeden 2021 e.a., p. 43.

68 Zowel omdat de geanalyseerde gegevens met strafvorderlijke opsporingsbevoegdheden worden vergaard, als omdat de geanalyseerde data aan de basis staan van nieuwe opsporingsonderzoeken waarin strafvorderlijk opsporingsbevoegdheden worden uitgeoefend op basis van uit de analyses voortvloeiende (nieuwe) verdenkingen.

het recht op bescherming van de persoonlijke levenssfeer – die het gevolg is van het overheidshandelen.[69]

Omdat bij datagedreven opsporing bevoegdheden op grond van een ander normeringskader dan geldend voor strafvorderlijke opsporingsbevoegdheden worden ingezet, moet daarom de aandacht uitgaan naar een normatieve verbinding tussen beide reguleringskaders.[70] Dat betekent dat in de normering tot uitdrukking zal moeten worden gebracht dat strafvorderlijke (basis)beginselen (ook) een rol dienen te spelen bij de bevoegdheidsuitoefening op grond van de Wpg in de context van datagedreven opsporing.[71] Op die wijze komt ook normatief tot uitdrukking dat het gehele palet aan bevoegdheidsuitoefening tot de opsporing moet worden gerekend. Dit betekent dat bijvoorbeeld vanuit het perspectief van de onschuldpresumptie, sprake dient te zijn van objectiveerbare feiten en omstandigheden op basis waarvan iemand subject van onderzoek wordt in het kader van of als uitvloeisel van de data-analyse.[72]

Kortom, er moet samenhang worden aangebracht in de normeringskaders (Wetboek van Strafvordering en Wpg). Voor het bewerkstelligen van normatieve samenhang bestaat bovendien nog een extra belangrijke aanleiding: ook vanuit het perspectief van het recht op bescherming van de persoonlijke levenssfeer dient de normering integrale bescherming te bieden en is een scheiding in de normering tussen bevoegdheden tot vergaring van data en bevoegdheden tot verwerking en analyse van data niet te maken.[73] Wij menen daarom – en pleitten daarvoor, net als anderen, al eerder[74] – dat data-analyses een grondslag vereisen in het Wetboek van Strafvordering *of* dat, *vice versa*, de uitoefening van analysebevoegdheden op grond van de Wpg nadere normering behoeft op grond van de (basis)beginselen van strafvordering.[75] Een dergelijke verbindende normering doet recht aan de verbreding van doelstellingen van het optreden in de opsporing. Dat maakt bovendien mogelijk dat de strafrechter – vanuit zijn controlerende taak in het concrete voorliggende strafproces – deze bepalingen in zijn beoordeling over de rechtmatigheid van de opsporing betrekt.[76] Op de (verdere) inrichting van dat toezicht zullen wij hierna nader ingaan.

69 Hirsch Ballin 2022-2, p. 25-28, 32 en 36 en Schermer & Galič 2022, p. 175-177.

70 In die zin ook: Fedorova e.a. 2022, p. 157-161 en Schermer 2022, p. 13.

71 Stevens e.a. 2021, p. 243-244.

72 Voor een nadere uitwerking van dergelijke strafvorderlijke basisbeginselen zie: Stevens e.a. 2021, p. 243-244. Zie ook Schermer & Oerlemans 2020, p. 19. Zie eerder ook het advies van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018), *Regulering van opsporingsbevoegdheden in een digitale omgeving* (hierna: Commissie Koops), sll., juni 2018, p. 28: *"De wetgever dient aandacht te besteden aan geautomatiseerde data-analyse in het moderniseringstraject in brede zin, en daarbij de mogelijkheid te overwegen in het Wetboek van Strafvordering de momenteel impliciete eis van uitlegbaarheid van strafvorderlijke beslissingen te expliciteren indien deze beslissingen (mede) op geautomatiseerde data-analyse worden gebaseerd."*

73 Dat is ook de conclusie die voortvloeit uit de rechtspraak van het EHRM en Hof van Justitie van de EU inzake onderzoek aan (bulk)data. Zie daarover Hirsch Ballin 2022-2, p. 30-32 en Schermer & Galič 2022.

74 M. Knapen, 'Privacyvraagstukken niet opgelost met nieuw wetboek' (interview M.F.H. Hirsch Ballin), *Mr.Online,* 10 december 2019, Hirsch Ballin 2022-2, Stevens e.a. 2021 en Schermer & Galič 2022.

75 Zie in vergelijkbare zin ook Schermer 2017, p. 214, Schermer & Galič 2022, p. 176 en Fedorova e.a. 2022, p. 160-161.

76 Zie HR 1 december 2020, ECLI:NL:HR:2020:1889, r.o. 2.1.3: *"[..] Toepassing van artikel 359a Sv kan ertoe strekken dat het recht van de verdachte op een eerlijk proces als bedoeld in artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM) wordt gewaarborgd. Daarnaast berust de beantwoording van de vraag of een rechtsgevolg aan een vormverzuim moet worden verbonden, en zo ja de wijze waarop dat gebeurt, in de kern op een afweging van belangen. Daarbij gaat het om de met vervolging en berechting van strafbare feiten gemoeide belangen – waaronder de belangen van waarheidsvinding en van de bestraffing van de daders van strafbare feiten – en de belangen die verband houden met de handhaving van grondrechten en de bevordering van een normconform verloop van het voorbereidend onderzoek."*

6. Toezicht en controle

Datagedreven opsporing richt zich óók op de verzameling van informatie voor andere, toekomstige onderzoeken en interventies ten aanzien slachtoffers of ter verstoring van criminele structuren. Dit brengt mee dat er slechts een beperkte rol is voor controle door de strafrechter.[77] Juist in cybercriminaliteitszaken blijkt er in de praktijk vaak geen zittingsrechter meer aan te pas komen die de rechtmatigheid van het opsporingsonderzoek controleert. Als bijvoorbeeld het doel is een cybercriminele (ICT-)infrastructuur onderuit te halen en het verdienmodel aan te tasten, dan is het nagestreefde effect van een andere aard dan het nemen van strafvorderlijke beslissingen en blijft het daarmee buiten het zicht van de strafrechter.[78]

Controle door de strafrechter zal door verschuiving van de doelstellingen van opsporing dus vaker geen rol spelen. Dat geldt te meer nu de controlerende taak van de strafrechter voor onrechtmatigheden begaan *buiten* de reikwijdte van het opsporingsonderzoek, beperkt is tot onrechtmatigheden die van bepalende invloed zijn geweest op het verloop van het opsporingsonderzoek naar en/of de (verdere) vervolging van de verdachte ter zake van het tenlastegelegde feit.[79] Het is illustratief dat voor de strafrechter in de cryptotelefoonzaken de naleving van de voorschriften van de Wpg niet relevant lijken te zijn:

> "De rechtbank heeft op 28 april 2021 al besloten dat de Wpg geen belangrijk strafvorderlijk voorschrift is. De verdediging heeft dan ook geen belang bij een toetsing aan de voorschriften van de Wpg. Deze toetsing is immers niet van belang voor de vragen die de rechtbank in het kader van de artikelen 348 en 350 Sv dient te beantwoorden, noch een vraag die beantwoord moet worden bij de toetsing of sprake is van een eerlijk proces als bedoeld in artikel 6 EVRM."[80]

Hiervoor is in paragraaf 5 al uiteengezet dat het daarom van belang is dat in de normering de verbinding tussen het Wetboek van Strafvordering en de Wet politiegegevens tot uitdrukking wordt gebracht. Daarbij komt dat de aandacht moet uitgaan naar de inrichting van het toezicht op de praktijk van datagedreven opsporing, gelet op dat normeringskader. Datagedreven opsporing raakt de fundamentele rechten van burgers, zowel in de uitoefening van hun recht op privacy als in de zin dat interventies van welke aard dan ook die worden gebaseerd op de uitkomsten van de analyses raken aan de onbelemmerde uitoefening van de fundamentele rechten.[81] Zoals hiervoor toegelicht kan van de strafrechter in dit verband niet veel worden verwacht. Een en ander brengt mee dat aanleiding bestaat voor herijking van de inrichting van toezicht op de uitoefening van strafvorderlijke opsporing.[82]

---

77 Vgl. de conclusie van de Procureur-Generaal bij de Hoge Raad in de op 9 november 2022 openbaar gemaakte eindrapportage van het thematisch onderzoek over de toepassing van de hackbevoegdheid: Procureur-Generaal bij de Hoge Raad der Nederlanden, *Onderzoek in een geautomatiseerd werk. Eindrapportage; Over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba, lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie,* Den Haag, september 2022, p. 3.

78 Zie ook J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017, nr. 4, p. 359 en Schermer 2022, p. 14.

79 HR 1 december 2020, ECLI:NL:HR:2020:1889, r.o. 2.2.2.

80 Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584. Zie in vergelijkbare bewoordingen of strekking ook: Rb. Oost-Brabant 15 december 2021, ECLI:NL:RBOBR:2021:6861 en Rb. Amsterdam 22 december 2021, ECLI:NL:RBAMS:2021:7553, r.o. 4.5.

81 Vgl. Hirsch Ballin 2022, p. 12-13 en 18.

82 Zie ook Commissie Koops 2018, p. 24, 30-31 en 62.

Steun daarvoor kan worden gevonden in het advies van de Afdeling Advisering van de Raad van State over de voorstellen voor een gemoderniseerd Wetboek van Strafvordering. De Raad van State kwam tot de conclusie dat voor de realisering van adequaat en effectief toezicht in de opsporing niet verder naar de strafrechter moet worden gekeken. Juist andere externe en interne controlemechanismen dienen een belangrijker rol te vervullen.[83] Wij menen dat de verschuiving in de doelstellingen van opsporing bij datagedreven opsporing, waardoor de impact van de vergaringsbevoegdheden op de fundamentele rechten niet los kan worden gezien van de analyse en het verdere gebruik van die data, nog duidelijker maakt dat adequaat en effectief toezicht op datagedreven opsporing niet alleen bij de strafrechter en bestaande toezichthoudende organen kan blijven liggen. In het bijzonder in de context van cybercrime-onderzoeken geldt dat te meer waar de vergaarde intelligence de basis vormt voor andersoortige reacties dan nieuwe opsporingsonderzoeken met het oog op vervolging en berechting van verdachten.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de Wpg en is aldus ook de bevoegde toezichthoudende autoriteit in de zin van de Richtlijn gegevensbescherming opsporing en vervolging.[84] Stevens e.a. stelden in 2021 al vast dat dit toezicht ten aanzien van verwerkingen voor rechtshandshavingsdoeleinden waarschijnlijk te kort zal schieten.[85] De AP kan gebruik maken van verschillende handhavende en sanctionerende bevoegdheden.[86] Zij kan bijvoorbeeld een last onder dwangsom of een bestuurlijke boete opleggen. De AP heeft echter geen bevoegdheid om bij vastgestelde onrechtmatigheden verwerkingen stil te leggen.[87]

Een belangrijk knelpunt ten aanzien van effectieve waarborgen en het toezicht op de naleving van de Wpg is dat onrechtmatigheden slechts naar boven komen als een individu een klacht indient.[88] Als de betrokkene echter niet wordt geïnformeerd, het recht op toegang tot informatie al te zeer wordt beperkt, of de politie een beroep doet op de bescherming van modus operandi, kan de betrokkene onvoldoende toegang hebben tot informatie over de gegevensverwerking die op hem of haar betrekking heeft. Dat betekent dat de controle op de naleving van het gegevensbeschermingsrecht in belangrijke mate afhankelijk is van een proactieve houding van de AP.[89] Uit de publicaties op de website van de AP blijkt echter dat de toezichthouder weinig actief is geweest wat betreft onderzoek naar gegevensverwerking door de politie, laat staan specifiek naar datagedreven opsporing.[90] Fedorova e.a. constateren in hun onderzoek naar strafvorderlijke gegevens:

> "In de praktijk heeft dit tot gevolg dat doorgaans niet uitvoerig wordt gecontroleerd of de Wpg en de daarin vervatte gegevensbeschermingsrechtelijke beginselen zijn nageleefd, nu dergelijke

83 Advies RvS Modernisering, deeladvies E, p. 196-197.

84 Richtlijn (EU) 2016/680 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.

85 Stevens e.a. 2021, p. 240-241.

86 Art. 35c Wpg.

87 Zie ook Stevens e.a. 2021, p. 240-241. Zie o.a. ook P. de Hert & J. Sajfert, 'The role of data protection authorities in supervising police and criminal justice authorities processing personal data', in: C. Brière & A. Weyembergh (red.), *The needed balances in EU Criminal Law: past, present and future*, London: Hart 2018, p. 251-252.

88 Zie voor andere knelpunten ook Stevens e.a. 2021.

89 Zie ook Stevens e.a. 2021, p. 240-241.

90 Het laatste nieuwsbericht over handhavend optreden van de AP gerelateerd aan de Wpg dateert van 22 februari 2019 naar aanleiding van een onderzoek uit 2017 ('Nationale Politie voldoet aan last onder dwangsom', *autoriteitpersoonsgegevens.nl*). Zie in vergelijkbare zin: Schermer & Galič 2022, p. 171.

schendingen toch vaak niet tot rechtsgevolg hoeven te leiden. Voorts wordt ook aangenomen dat het niet tot de taak van de strafrechter behoort om de opsporing te controleren. De AP lijkt deze rol ook niet voor haar rekening te kunnen nemen, nu deze autoriteit vooral systeemtoezicht houdt en niet op concrete strafzaken".[91]

Verder houdt de procureur-generaal bij de Hoge Raad 'thematisch toezicht' op het openbaar ministerie. De procureur-generaal kan daarbij de minister 'in kennis kan stellen van het feit dat naar zijn oordeel het Openbaar Ministerie bij de uitoefening van zijn taak de wettelijke voorschriften niet naar behoren handhaaft of uitvoert'.[92] Deze taak kan echter evenmin worden gezien als een volwaardige vorm van toezicht op het gebruik van data-analyses in het kader van de opsporing.[93] De onderzoeken zijn thematisch, dienen betrekking te hebben op de volle breedte van de taken van het openbaar ministerie (en tegelijkertijd dus niet op die van de politie) en de procureur-generaal beschikt niet over de capaciteit om meerdere thema's naast elkaar te onderzoeken.

Tot slot is de Inspectie Justitie en Veiligheid op grond van artikel 65 Politiewet 2012 belast met het toezicht op de taakuitvoering door de politie, maar heeft de Inspectie geen taak ten aanzien van het openbaar ministerie. De Inspectie is daarnaast in het bijzonder belast met toezicht op de uitoefening van de hackbevoegdheid (ex art. 126nba lid 1, 126uba lid 1 en 126zpa lid 1 Sv).[94] De focus ligt daarbij op de uitvoering van de procedureregels in onderliggende besluiten. De focus ligt dus niet op de rechtmatigheid van het onderzoek, zoals naleving van principes als noodzakelijkheid en proportionaliteit in concrete zaken. Bovendien kan worden afgevraagd of een inspectie die is ingebed bij het ministerie van Justitie en Veiligheid kan worden aangemerkt als een voldoende onafhankelijke autoriteit[95] voor het uitoefenen van toezicht op datagedreven opsporing.[96]

Vastgesteld moet dan ook worden dat het huidige stelsel van toezicht en controle onvoldoende recht doet aan en niet is toegesneden op de praktijk van datagedreven opsporing. Fedorova e.a. komen ook tot deze conclusie:

"In de kern is het probleem dat weliswaar verschillende onafhankelijke en niet-onafhankelijke toezichtsorganen toezicht kunnen houden op de verwerking van gegevens voor strafvorderlijke doeleinden, maar dat vanwege de taakopvatting en verschillende capaciteitsoverwegingen niet daadwerkelijk van effectief toezicht kan worden gesproken. Bij het nadenken over een nieuwe systematiek of andere inhoudelijk normering, kan een nadere reflectie op het toezicht dus niet achterwege blijven."[97]

91 Fedorova e.a. 2022, p. 168.
92 Zie Artikel 122 lid 1 van de Wet op de rechterlijke organisatie (Wet RO) en zie de webpagina 'Toezicht op het Openbaar Ministerie', laatstelijk geraadpleegd op 28 juni 2022.
93 Zo ziet de P-G bij de Hoge Raad het ook zelf, zie Eindrapportage Procureur-Generaal bij de Hoge Raad 'Onderzoek in een geautomatiseerd werk' 2022 (zie voetnoot 76), p. 6.
94 Zie het hiervoor genoemde rapport van de P-G bij de Hoge Raad.
95 Vgl. Opinie P. Omtzigt, R. Torenvlied, C. Aarts, M. Stahlie, 'Maak de rijksinspecties écht onafhankelijk', *FD* 26 juni 2022.
96 Zo ook de P-G bij de Hoge Raad, Eindrapportage Procureur-Generaal bij de Hoge Raad 'Onderzoek in een geautomatiseerd werk' 2022 (zie voetnoot 76), p. 6.
97 Fedorova e.a. 2022, p. 168. Zie in vergelijkbare zin Schermer & Galič 2022, p. 175: "Met betrekking tot de rechtsbescherming leidt dit ons tot de conclusie dat er geen effectief toezicht is op de naleving van de Wpg in individuele zaken."

Wij menen dat de met datagedreven opsporing gepaard gaande verbreding van doelstellingen van de opsporing én de daarvoor gevonden grondslagen voor het optreden, daarom ook meebrengen dat wordt gezocht naar een andere, nieuwe vorm van onafhankelijk toezicht op de opsporing. In navolging van Fedorova e.a. denken wij daarbij niet direct aan een meer nadrukkelijke rol van de rechter-commissaris. De analyse van gegevens is een dynamisch proces dat zich niet goed leent voor toestemming vooraf door een rechter-commissaris of onafhankelijke instantie.[98] Juist de mogelijkheid mee te denken, 'real-time' mee te kijken en te interveniëren zijn ingrediënten voor effectief toezicht door een onafhankelijke, meer gespecialiseerde, instantie.[99]

Ook denken wij niet aan het doorvoeren van verbeteringen op het toezicht door de procureur-generaal bij de Hoge Raad en het Openbaar Ministerie.[100] Wij achten die oplossing onvoldoende voor de controle op het gebruik van data-analyses, in het bijzonder gelet op de strenge (en steeds strenger wordende) eisen in de rechtspraak van het EHRM en het HvJ van de EU wat betreft de controle op inzet van digitale bevoegdheden in het licht van de bescherming van de persoonlijke levenssfeer.[101] Bij de verwerking van bulkgegevens gaat het bijvoorbeeld om toezicht door een onafhankelijke autoriteit *in alle fasen* van gegevensverwerking, waarbij de noodzaak en proportionaliteit in concrete gevallen kan worden getoetst.[102]

Gelet op het voorgaande menen wij dat het nodig zal zijn het stelsel van toezicht en controle op datagedreven opsporing her in te richten.[103] Wij kunnen ons goed voorstellen dat dit heeft te betekenen dat een nieuwe vorm van toezicht op de inzet van data-analyses in of ten behoeve van de politietaken (inclusief de opsporing en aldus de datagedreven opsporing) wordt gerealiseerd door de oprichting van een onafhankelijk extern toezichtsorgaan. Dit toezichtsorgaan zou dan als toezichthouder in de zin van de Richtlijn gegevensbescherming opsporing en vervolging dienen te fungeren en daarnaast in bredere zin (dan het gegevensbeschermingsrecht) een controlerende taak moeten hebben ten aanzien van datagedreven opsporing.[104] Denkbaar zou zijn dat het toezicht wordt ondergebracht bij een externe Commissie van Toezicht, vergelijkbaar met de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

7. Conclusie en aanbevelingen

Datagedreven onderzoek is een 'game changer' voor de politie en dat zou het ook voor de relatie tussen Sv en Wpg en het bijbehorende toezicht dienen te zijn. In dit artikel hebben

98 J.J. Oerlemans, 'Metadata-analyse in de Wiv 2017', *Privacy & Informatie* 2020, nr. 6, p. 263.

99 Zie ook Fedorova e.a. 2022, p. 170-172.

100 Zie: M. Samadi, *Normering en toezicht in de opsporing: Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen* (diss. Leiden), 2020, p. 403-404.

101 Zie uitvoeriger: M.F.H. Hirsch Ballin en M. Galič, 'Digital investigation powers and privacy. Recent ECtHR case law and implications for the modernisation of the Code of Criminal Procedure', *Boom Strafblad* 2021/4, m.n. p. 153-154 en Schermer & Galič 2022, p. 171-175.

102 Zie bijvoorbeeld *Big Brother Watch and others*, § 356. Uit HvJ EU 2 maart 2021 (*Prokuratuur*), C-746/18, ECLI:EU:C:2021:152, § 51-56 volgt dat het Openbaar Ministerie niet als een onafhankelijke instantie kan worden gezien voor de toetsing vooraf van toepassing van vorderingsbevoegdheden.

103 In navolging van Schermer 2017 en als uitwerking en opvolging van aanbevelingen 1, 4, 5 en 11 van de Commissie-Koops 2018.

104 Zie in vergelijkbare zin Commissie-Koops 2018, p. 30-31, M. Devroe, 'Is het totaal meer dan de som der delen? Toezichtsvormen op strafvorderlijk overheidsoptreden', *NJB* 2017/2278. Hirsch Ballin 2022, p. 20, Stevens e.a. 2021, p. 243 en Fedorova e.a. 2022, p. 170-171.

wij in paragraaf 2 het model van datagedreven opsporing beschreven en geïllustreerd aan de hand van de daarover bekende strafrechtspraak en de praktijk bij het Team High Tech Crime van de politie. De cryptotelefoon-operaties laten zien dat het model van het Team High Tech Crime ook wordt toegepast in andere strafzaken, buiten de context van de cybercriminaliteit. Vastgesteld kan worden dat de intelligencepraktijk inmiddels verweven is geraakt met de opsporingspraktijk. Dit legt druk op het huidige stelsel van strafvordering.

De verzameling van de gegevens bij datagedreven opsporing vindt plaats met toepassing van bijzondere opsporingsbevoegdheden die worden gereguleerd in het Wetboek van Strafvordering. Uit paragraaf 3 blijkt dat de verwerking en analyse van deze gegevens plaatsvindt op grond van de Wpg en dat de daaropvolgende interventie een nieuw opsporingsonderzoek kan betreffen, maar bijvoorbeeld ook 'verstoring' met een grondslag in de Politiewet. In paragraaf 4 en 5 hebben wij toegelicht dat deze praktijk een normatieve verbinding vergt tussen de reguleringskaders.

Het spanningsveld van datagedreven opsporing met de (traditionele) uitgangspunten van het stelsel van strafvordering, laat zien dat enerzijds moet worden erkend dat de toepassing van opsporingsbevoegdheden óók gericht kan zijn op andere doelstellingen (zoals het verstoren van criminele infrastructuren of het produceren van intelligence) en anderzijds dat wordt gezocht naar een vorm van normering die ook aansluit bij die andere doelstellingen. Wij achten daarvoor in de eerste plaats van belang dat een keuze wordt gemaakt voor óf normering van data-analyses in het Wetboek van Strafvordering óf voor nadere normering van analysebevoegdheden in de Wpg. Daarbij moet recht worden gedaan aan (basis)beginselen van strafvordering zodat de verbinding tussen de normeringskaders wordt gelegd.

De totstandkoming van het nieuwe Wetboek van Strafvordering biedt de ruimte om op een weloverwegen manier te komen tot een herpositionering van de opsporing en, in het bijzonder, de relatie daarin tussen strafvorderlijke bevoegdheidsuitoefening en de uitoefening van (analyse)bevoegdheden binnen de reikwijdte van de opsporing die recht doet aan de praktijk van datagedreven opsporing en de impact voor de rechten van burgers die daarmee gepaard gaat. Die herpositionering houdt wat ons betreft in dat (meer of meer expliciete) ruimte bestaat voor andere dan de (traditionele) doelstelling van opsporing, maar dit tegelijkertijd moet betekenen dat nadrukkelijker de relatie wordt gelegd tussen beginselen van strafprocesrecht en normering van vergaringsbevoegdheden en grondslagen in de Wpg voor het verdere verwerken van vergaarde gegevens voor andere doeleinden.

Ruimte bieden voor bredere doelstellingen, betekent echter ook dat in de normering de bakens moeten worden verzet. Daarvoor zal het nodig zijn het stelsel van toezicht en controle op datagedreven opsporing her in te richten. Wij kunnen ons goed voorstellen dat dit heeft te betekenen dat een nieuwe vorm van toezicht op de inzet van data-analyses in of ten behoeve van de politietaken (inclusief de opsporing en aldus de datagedreven opsporing) wordt gerealiseerd door de oprichting van een onafhankelijk extern toezichtsorgaan. Dit toezichtsorgaan zou dan als, gespecialiseerde, toezichthouder in de zin van de Richtlijn gegevensbescherming opsporing en vervolging dienen te fungeren en daarnaast in bredere zin (dan het gegevensbeschermingsrecht) een controlerende taak moeten hebben ten aanzien van datagedreven opsporing.

Ten slotte is het van belang dat expliciet wordt onderkend voor welke doeleinden data-analyses kunnen worden gebruikt. Juist de totstandbrenging van een nieuwe onafhankelijke

toezichthouder maakt naar onze mening goed voorstelbaar dat het voortaan ook (expliciet) kan gaan om andere doelen en reacties dan die behorend bij de traditionele strafvorderlijke oriëntatie van strafvorderlijk bevoegdheidsuitoefening op bewijsvergaring. De totstandbrenging van een andere vorm van toezicht in de verbinding tussen strafvorderlijke bevoegdheden tot vergaring van data en de verwerking en analyse ervan (de intelligence-functie) op grond van de Wpg, betreft een significante verandering voor de opsporingspraktijk en het stelsel van toezicht en controle op strafvorderlijk optreden. Toch is het een noodzakelijke aanvulling om de ontstane vervlechting van inlichtingen en opsporing van een passende normatieve basis te voorzien.