PELS RIJCKEN

Geautomatiseerde data-analyse in het nieuwe Wetboek van Strafvordering

prof. mr. M.F.H. (Marianne) Hirsch Ballin

1. Inleiding

De sterke ontwikkeling van de technologie is een van de door de regering genoemde (kern)ontwikkelingen die ten grondslag liggen aan het nieuwe Wetboek van Strafvordering. De beschikbaarheid van nieuwe technieken heeft ervoor gezorgd dat de wijze waarop de strafvordering plaatsheeft, is gemoderniseerd en nog verder kan en zal worden gemoderniseerd.[1] Het gaat dan in het bijzonder om digitale opsporingsmethoden. Diverse (met name) digitale bevoegdheden hebben in de loop der jaren al een plek gekregen in het huidige Wetboek van Strafvordering, onder meer op grond van de wetten Computercriminaliteit I-III. Dit is de overzichtelijkheid van de regeling van opsporingsbevoegdheden niet ten goede gekomen. Het nieuwe Strafvordering voorziet in Boek 2 daarom in een vereenvoudigde en opnieuw gestructureerde regeling voor de

opsporing, waarin het onderzoek van gegevens een centrale plek heeft gekregen. Daarnaast bevatten de voorstellen bepalingen met specifieke grondslagen voor digitale onderzoeksbevoegdheden, zoals het openbronnenonderzoek, de mogelijkheid van netwerkzoeking[2] en de nieuwe regeling van het onderzoek van gegevens. De digitale opsporing heeft zo in het nieuwe Wetboek een stevige plek gekregen. Dat biedt zowel praktijk als burger meer rechtszekerheid.

Parallel aan het toegenomen belang van de inzet van digitale opsporingsbevoegdheden heeft de analyse van grote hoeveelheden vergaarde data de opsporingspraktijk significant veranderd. Opsporing is steeds meer datagedreven.[3] Doordat de inzet van digitale methoden er veelal toe leidt dat gegevens in bulk worden vergaard (denk bijvoorbeeld aan de data van cryptotelefoonservers als Ennetcom, EncoChat, SkyECC en Exclu), zijn die data eerst goed bruikbaar ten behoeve van de opsporing *na* analyse. Voorts levert de inzet van geavanceerde analysetechnieken – die bovendien nog volop in ontwikkeling zijn – ten opzichte van de oorspronkelijke data, nieuwe – geconstrueerde of gereconstrueerde – informatie op.[4] Ook in dat opzicht, en door de combinatie van beide factoren, is de (geautomatiseerde) analyse een van de belangrijkste ontwikkelingen in de opsporing, waarvan we de uiteindelijke potentie en impact nu nog niet kunnen overzien.

Naar (aspecten van) de normering van digitale opsporingsbevoegdheden is de afgelopen jaren al veel onderzoek gedaan.[5] In het bijzonder het onderzoek van de Commissie-Koops[6] is richtinggevend geweest voor de regeling in de voorstellen van het nieuwe Wetboek van Strafvordering. Opvallend tegen de achtergrond van het grote (en naar verwachting toenemende) belang van data-analyse voor de opsporing is dat de normering van bevoegdheden tot analyse in het nieuwe Wetboek van Strafvordering nog relatief onderbelicht is gebleven. Het is daarom dat in dit themanummer onze aandacht in het bijzonder uitgaat naar aspecten verbonden aan die bevoegdheden.

Daarbij gaat het in de eerste plaats om data-analyse van vergaarde (bulk)data door de opsporingsautoriteiten. Door de inzet van opsporingsbevoegdheden kunnen grote hoeveelheden data worden verkregen. In het gemoderniseerde Wetboek van Strafvordering wordt (vooralsnog) vastgehouden aan de gescheiden regeling van bevoegdheden tot vergaring van data (in het Wetboek van Strafvordering) en bevoegdheden tot analyse en verdere verwerking van (de vergaarde) data (in de Wet politiegegevens). De vraag is in hoeverre dit onderscheid in de context van digitale opsporing en het belang en de impact

van gegevensanalyse nog houdbaar is. In de tweede plaats vragen wij aandacht voor een in het nieuwe Wetboek van Strafvordering geïntroduceerde nieuwe bevoegdheid tot het laten uitvoeren van de gegevensanalyse door derden, voorafgaand aan de verstrekking. Op de vraagstukken verbonden met beide situaties van data-analyse in het kader van de opsporing ga ik hierna, en ter introductie van de hiernavolgende bijdragen van Huisman en Stal, nader in.

2. Geautomatiseerde data-analyse door de opsporing

Het nieuwe Wetboek van Strafvordering voorziet niet in bevoegdheden tot analyse van vergaarde data; de normering van analyse van vergaarde politiegegevens blijft volgens de toelichting een onderwerp dat regeling vindt in de Wet politiegegevens. Aanvankelijk was de gedachte dat parallel aan het nieuwe Wetboek van Strafvordering ook een nieuwe gegevensbeschermingswet voor politie en justitie zou worden ontworpen.[7] Omdat net als de implementatie van het nieuwe Strafvordering, de implementatie van een dergelijke nieuwe gegevensbeschermingswet voor in het bijzonder de politie en andere opsporingsdiensten een enorme opgave zal zijn die lastig gelijktijdig kan plaatsvinden, is van gelijktijdige totstandkoming afgezien.[8] De vraag is echter of dat ook kan betekenen dat in het licht van de totstandkoming van het nieuwe Strafvordering de normering van bevoegdheden tot analyse van (grote hoeveelheden) data geen nadere aandacht behoeft. Juist omdat in de huidige digitale opsporingspraktijk veel vaker grote hoeveelheden data worden vergaard (en de vergaring dus ongerichter is), is de analyse ervan de stap in het opsporingsproces die de meeste impact heeft op de rechten en vrijheden van burgers.[9] De gescheiden normering tussen vergaring en verwerking kan in de digitale opsporingspraktijk tot gevolg hebben dat het recht op bescherming van de persoonlijke levenssfeer alsook de bescherming van strafvorderlijke basisbeginselen in de knel komen; althans in een normeringsvacuüm terechtkomen.[10] Het gaat er dan bijvoorbeeld om dat bij de beoordeling (door de rechter-commissaris of de officier van justitie; alsook achteraf door de zittingsrechter) van de proportionaliteit en subsidiariteit van de inzet van een opsporingsbevoegdheid niet wordt meegenomen wat er na de vergaring met die data gebeurt en dat bij gebruik van data na analyse op grond van de Wet politiegegevens in een nieuwe strafzaak de rechtmatigheid van die analyse in de regel geen rol meer zal spelen.[11] Bij de totstandbrenging van een nieuwe regeling voor de normering van de bevoegdheden tot vergaring dient de impact van de analyse van de vergaarde data dan ook in ogenschouw te worden genomen. Daarbij komt ook de vraag op of het niet passender is

(bepaalde) bevoegdheden tot analyse een plek te geven in het Wetboek van Strafvordering in plaats van in de Wet politiegegevens.[12] Op zichzelf wordt de noodzaak tot nadere overdenking van de normering van de analyse (verwerking) van grote hoeveelheden in de opsporing vergaarde data in de memorie van toelichting onderkend, maar wordt de richting waarin de normering zich zou moeten begeven in afwachting van de verdere ontwikkeling van de Europese rechtspraak uitgesteld tot het aanvullingsspoor.[13]

Bij die stand van zaken is er alle reden aandacht te geven aan en nader onderzoek te doen naar het in de literatuur al herhaaldelijk gesignaleerde 'normeringsgat' of onvoldoende samenhangend normeringskader (met *end-to-end safeguards*[14]) tussen de strafvorderlijke bevoegdheden en de bevoegdheden tot verwerking op grond van de Wet politiegegevens. In opdracht van het WODC hebben wetenschappers van de Radboud Universiteit onderzoek verricht naar de strafvorderlijke gegevensverwerking.[15] De minister acht de uitkomsten van dat onderzoek – zo volgt uit de memorie van toelichting – thans nog onvoldoende om de uiteindelijke richting van de normering te bepalen. Dat neemt niet weg dat het Nijmeegse onderzoek belangrijke aanknopingspunten geeft voor via het aanvullingsspoor nog aan het nieuwe Wetboek van Strafvordering toe te voegen bepalingen die betrekking hebben op analyse (door de opsporing) van vergaarde data. Vertrekpunt dient volgens de Nijmeegse onderzoekers te zijn dat 'verwerkingshandelingen die zijn gericht op kennisvermeerdering én een strafvorderlijk doel dienen' in het Wetboek van Strafvordering moeten worden geregeld. 'Overige verwerkingshandelingen' kunnen in de Wet politiegegevens worden genormeerd.[16] Dit onderscheid spreekt op zichzelf aan. Tegelijkertijd zal het lastig zijn deze verwerkingshandelingen met een strafvorderlijk doel goed te scheiden van bedoelde 'overige' verwerkingshandelingen. Of misschien nog sterker: het is de vraag of deze handelingen überhaupt zijn te scheiden, omdat ook 'overige verwerkingshandelingen' het sluitstuk zullen zijn (of een nieuw beginpunt zijn) van de ingreep in de rechten en vrijheden van burgers en daarmee binnen het bereik van bedoelde *end-to-end safeguards* vallen. In andere woorden: omdat de rechtsbetrekkingen vervlochten zijn, zal een procesrechtelijke verbinding moeten worden bewerkstelligd tussen de bevoegdheden tot vergaring en de bevoegdheden tot verdere verwerking in de Wet politiegegevens, bijvoorbeeld door overstijgend toezicht te bewerkstelligen. In het kader van dat toezicht zou de aandacht dan ook moeten uitgaan naar de proportionaliteit van de verdere verwerking in relatie tot het oorspronkelijke doel van de vergaring van de data.[17]

Hoe dan ook – zowel voor een eventuele normering van bepaalde verwerkingshandelingen via het aanvullingsspoor in Strafvordering als voor het bewerkstelligen van de benodigde met de Wpg verbindende normering (bijv. via het toezicht) – is eerst van belang dat het proces (vergaring-analyse-verder gebruik) door iedereen goed wordt begrepen. Dat proces omvat de verwevenheid van en implicaties voor de betrokken rechten en belangen – en welke (kring van) personen aldus bescherming behoeven – bij de verdere verwerking door analyse. Het is daarom dat in de volgende bijdrage Huisman nader ingaat op de aard, mogelijkheden en impact van data-analyse.[18]

3. Geautomatiseerde data-analyse door derden

De tweede voor dit thema relevante bevoegdheid betreft de voorgestelde nieuwe bevoegdheid tot het laten verrichten van een data-analyse door *derden*. Anders dan de data-analyse door de opsporingsautoriteiten zelf, heeft deze bevoegdheid – als ik het goed zie – nog in het geheel geen nadere aandacht gekregen. Op grond van artikel 2.7.50 nieuw Strafvordering kan de officier van justitie bedrijven of instellingen bevelen dat zij gegevens bewerken en het resultaat aan de officier van justitie verstrekken.

Artikel 2.7.50 nieuw Strafvordering[19] luidt:

1. In geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van vier jaar of meer is gesteld, kan de officier van justitie de persoon die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt en van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens, bevelen dat hij deze gegevens bewerkt en de daardoor verkregen gegevens verstrekt.
2. Indien het bevel betrekking heeft op een persoon die aanspraak kan maken op bronbescherming als bedoeld in artikel 1.6.8 of op communicatie die wordt beschermd door het telecommunicatiegeheim kan de officier van justitie het bevel alleen geven na een daartoe verleende machtiging van de rechter-commissaris. Artikel 1.6.8, tweede lid, is van overeenkomstige toepassing.
3. De officier van justitie kan in het bevel bepalen dat degene tot wie het bevel is gericht, de bewerking in overeenstemming met de aanwijzingen van de opsporingsambtenaar uitvoert.
4. De officier van justitie kan de in het eerste lid bedoelde persoon bevelen inlichtingen te verstrekken over de gegevens waartoe hij toegang heeft en over de handelingen die nodig zijn om de in het eerste lid bedoelde bewerking uit te voeren.

De bevoegdheid wordt in de eerste plaats van belang geacht om de verstrekking van gegevens gerichter te maken en aldus de ingreep in de persoonlijke levenssfeer geringer te maken. De omvang van de dataset waarover de opsporing de beschikking krijgt, is dan immers beperkter en meer afgebakend (gerichter). Ook brengt dat capaciteitsvoordelen voor de opsporing met zich mee: de (grote) bedrijven die beschikken over grote hoeveelheden gegevens (de memorie van toelichting noemt Google, Facebook en Apple) zouden veel beter zijn toegerust op het analyseren van de gegevens dan de opsporing.[20] Tegelijkertijd dient de belasting die een analysebevel voor het bedrijf oplevert door de officier van justitie te worden meegewogen in de beoordeling van de proportionaliteit en subsidiariteit. Daarover wordt opgemerkt dat kleinere bedrijven een relatief grotere inspanning zullen moeten leveren om de bewerking uit te voeren op hun dataset, dan grotere bedrijven, bij wie dergelijke data-analyses vaker voorkomen.[21]

Op grond van het tweede lid van art. 2.7.50 dient een machtiging van de rechter-commissaris te worden verkregen als het bevel betrekking heeft op een persoon die aanspraak kan maken op bronbescherming of op communicatie die wordt beschermd door het telecommunicatiegeheim. De NOvA heeft in haar advies over het voorstel voorts zorgen geuit over de waarborging van het verschoningsrecht in het geval van een bevel op grond van art. 2.7.50. In reactie daarop wordt in de toelichting erop gewezen dat, net als bij ‘gewone’ gegevensvorderingen bij een ander persoon dan een functioneel verschoningsgerechtigde, in het geval van een redelijk vermoeden dat het bevel zich uitstrekt tot gegevens waarop het functioneel verschoningsrecht van toepassing is, de regeling op grond van de artikelen 2.7.65 en 2.7.66 zal moeten worden toegepast. Dat betekent (eveneens) dat de rechter-commissaris in het geval van zo’n redelijk vermoeden moet worden betrokken en dat de rechter-commissaris dient te beslissen over de voorwaarden waaronder de bewerking moet plaatsvinden.[22] Hoe dat in de praktijk uitwerking zou moeten krijgen en of het überhaupt zal gebeuren dat deze bevoegdheid - betrekking kan hebben op verschoningsgerechtigd materiaal, wordt niet duidelijk. Dat komt ook doordat nog onvoldoende inzichtelijk is wat de aard is van de voorgenomen analyse en op wat voor gegevens – bijvoorbeeld ook de inhoud van communicatie, zoals e-mails? – die analyse betrekking heeft.

Het derde lid van art. 2.7.50 voorziet ten slotte in de bevoegdheid van de officier van justitie om aanwijzingen te geven voor de bewerking van de data. Die aanwijzingen worden in de toelichting vooral in verband gebracht met het stellen van eisen aan de uitvoering van de bewerking en de controleerbaarheid ervan achteraf. Ook kan een aanwijzing inhouden dat de bewerking dient te worden uitgevoerd in aanwezigheid van of onder toezicht van een opsporingsambtenaar of een deskundige. Ook kan in het licht van zo'n aanwijzing hardware en software ter beschikking worden gesteld voor de analyse.[23]

De voorgestelde nieuwe bevoegdheid tot data-analyse door een derde doet dus de vraag opkomen aan wat voor type analyse moet worden gedacht en op wat voor gegevens die analyse mogelijk betrekking heeft. De memorie van toelichting verschaft daarin niet veel inzicht. Wel wordt opgemerkt dat de bevoegdheid niet op iedere vorm van bewerking betrekking heeft. Het gaat om 'bewerkingen die verdergaan dan meervoudige zoekhandelingen, bijvoorbeeld het integraal met elkaar vergelijken van alle gegevens uit een dataset met alle gegevens uit een andere dataset, om zo gegevens te identificeren die in beide sets voorkomen'.[24] Belangrijkste kenmerk van de bevoegdheid is, aldus de toelichting, dat de bewerking 'nieuwe gegevens' oplevert die vervolgens worden verstrekt. Het is juist in dat verband dat ook belangrijke vragen over de aard van deze bevoegdheid opkomen. Zijn er beperkingen aan de aard van de technologieën, bijvoorbeeld de inzet van kunstmatige intelligentie, die voor het uitvoeren van de analyse worden ingezet? Hoe moeten we de (aanvullende) ingreep in de persoonlijke levenssfeer waarderen in vergelijking met een bevel tot verstrekking van de oorspronkelijke gegevens, gelet op de omstandigheid dat het toepassen van de analyse leidt tot 'nieuwe gegevens'? In dat verband zou er bijvoorbeeld aan kunnen worden gedacht het stelselmatigheidscriterium een positie te geven in de normering.[25]

In het verlengde hiervan komen vragen op over de controleerbaarheid van de betrouwbaarheid en rechtmatigheid van de uitkomsten van de analyse. Dienen de handelingen die door de bedrijven of instellingen worden verricht nader te worden gereguleerd, bijvoorbeeld naar aanleiding van de op korte termijn te verwachten Verordening tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie[26]? Zijn de mogelijkheden voor toezicht afdoende geborgd door de bevoegdheid van de officier van justitie om in dat verband aanwijzingen te geven? Dient de positie van de verdediging wat betreft het controleren van de betrouwbaarheid van de uitkomsten van de analyse te worden versterkt? De bijdrage van Stal laat aan de hand van

voorbeelden uit de huidige opsporingspraktijk zien in welke gevallen een bevel tot data-analyse een zinvolle bijdrage kan leveren aan de opsporing. Dat inzicht draagt ook bij aan het begrip van de aard van deze analyse en aldus aan de wijze waarop deze vragen zouden kunnen worden geadresseerd. Ook daarvoor doet zij in haar bijdrage een voorzet. Daarnaast is van belang dat we wat betreft de mogelijkheden van deze bevoegdheid de blik ook op de verdere toekomst richten. Gelet op de omvang van data die aanwezig kunnen zijn bij private partijen en de (ontwikkeling van de) technologische mogelijkheden van analyse, is de impact van deze bevoegdheid in potentie groot. Het is daarom van belang dat die potentie afdoende wordt begrepen om op die basis te kunnen komen tot een passende normering.

4. Afsluiting

De praktijk laat zien dat mogelijkheden die bevoegdheden tot data-analyse bieden voor de opsporing van groot belang zijn. De verdere ontwikkeling van de techniek zal die mogelijkheden alleen nog maar verder vergroten, en het belang ervan voor de opsporing evenzeer. Nu al is zichtbaar dat juist data-analyse een bevoegdheid van een fundamenteel andere aard is dan bevoegdheden waarmee vaststaande data worden verkregen. De analyse kan leiden tot 'nieuwe feiten' en 'nieuwe inzichten' ten opzichte van de oorspronkelijk vergaarde data. Dat maakt ook dat de rechten en vrijheden van een bredere kring van personen dan de verdachte of andere personen waarop de opsporing zich richt (bijvoorbeeld op grond van aanwijzingen van een strafbaar feit), door de toepassing van analysebevoegdheden kan worden geraakt. Dat maakt duidelijk dat het onderwerp in het kader van het aanvullingsspoor nog de nodige aandacht verdient. Deze inleiding en de bijdragen van Huisman en Stal geven daarvoor een aanzet.

Noten

1 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 9.

2 Reeds ingevoerd bij de Innovatiewet Strafvordering; art. 557 Sv.

3 Zie M.F.H. Hirsch Ballin en J.J. Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden', *DD* 2023, afl. 2; R.M. te Molder e.a., 'Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing', *Computerrecht* 2023/64.

4 M.F.H. Hirsch Ballin, 'Als een spin in het web voor de bestrijding van terrorisme en zware ondermijnende criminaliteit', *TvCr* 2022, afl. 2, p. 11; A.J. van Eeden, J.J. van Berkel

e.a., *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*, WODC Cahier 2021, afl. 23, p. 40.

5 Zie bijv. R.S. Veen, 'Digitale opsporing. Het EHRM en het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen', *DD* 2019, afl. 30; D.A.G. van Toor, 'Het nemo-teneturbeginsel bij digitale opsporingsbevoegdheden: oproep tot discussie over fundamentele bezinning van de normering van het opsporingsonderzoek in een digitale context', *TBSH* 2021, afl. 2; Hirsch Ballin en Oerlemans 2023; 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, afl. 4; L. Stevens, 'Over vangnetbepalingen voor de opsporing', *DD* 2021, 67.

6 Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.

7 *Kamerstukken II* 2013/14, 33842, nr. 2, p. 3 en zie ook nog het concept van de memorie van toelichting nieuw Wetboek van Strafvordering, ambtelijke versie juli 2020 (zie https://open.overheid.nl/documenten/ronl-905eeb75-f4c4-460c-9104-c5d87b51a5db/pdf), p. 228.

8 Zie *Kamerstukken II* 2021/22, 32761, nr. 218 en *Kamerstukken II* 2022/23, 36327, nr. 3 (Memorie van toelichting bij de vaststellingswet voor het nieuwe Wetboek van Strafvordering), p. 71 en zie Commissie implementatie nieuw Wetboek van Strafvordering (Commissie Letschert), 'Implementatiestrategie – eindrapportage', p. 3, bijlage bij *Kamerstukken II* 2020/21, 29279, nr. 637.

9 Vgl. Te Molder e.a. 2023, p. 111.

10 Hirsch Ballin en Oerlemans 2023, p. 32; B.W. Schermer, De gespannen relatie tussen privacy en cybercrime (oratie Leiden) 2022, verkregen via https://hdl.handle.net/1887/3484256; J.J. Oerlemans en B. Schermer, 'Antwoorden op prejudiciële vragen in Encrochat- en SkyECC-zaken, *Nederlands Juristenblad* 2023, afl. 31, p. 2610-2618.

11 Zie bijv. Gerechtshof Arnhem-Leeuwarden 16 november 2022, ECLI:NL:GHARL:2022:9878.

12 De vraag of de huidige bepalingen van de Wet politiegegevens voldoende normering bieden voor de huidige technische mogelijkheden tot analyse van (gecombineerde) politiegegevens laat ik verder rusten. Herhaaldelijk is er al op gewezen dat de grondslagen in de Wet politiegegevens voor dergelijke analyses niet voldoen. Zie Te Molder e.a. 2023, p. 111; B.W. Schermer en M. Galič, 'Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?', *NTS* 2022, afl. 3; L. Stevens e.a., 'Strafvorderlijke normering van

preventief optreden op basis van datakoppeling. Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond', *TBSH* 2021, afl. 4.

13 Dat is het wetgevingsspoor van de moderniseringsoperatie waarbij het huidige voorstel voor het nieuwe Wetboek van Strafvordering wordt aangevuld.
Zie *Kamerstukken II* 2022/23, 36327, nr. 3, p. 60 en 72.

14 Term ontleend aan EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24690/15, par. 350: 'Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime [...].'

15 M.I. Fedorova e.a., *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Nijmegen: Radboud University Press 2022.

16 Te Molder e.a. 2023, p. 112.

17 Vgl.: M.F.H. Hirsch Ballin, *Responsief strafprocesrecht in een netwerk van rechtsbetrekkingen' (Preadvies CJV 2022)*, Zutphen: Uitgeverij Paris 2023; Hirsch Ballin 2022; Hirsch Ballin en Oerlemans 2023.

18 Zie voorts W. Huisman, 'Slimmer strafrecht? Het MIT en de data gedreven opsporing', *DD* 2022, afl. 14.

19 *Kamerstukken II* 2022/23, 36327, nr. 2, p. 99.

20 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 610-611.

21 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 611.

22 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 612.

23 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 613.

24 *Kamerstukken II* 2022/23, 36327, nr. 3, p. 612.

25 Vgl. Commissie-Koops, p. 183 en 'Inhoudelijke rapportage Boek 2: Het opsporingsonderzoek (Project bijstand Tweede Kamer modernisering Wetboek van Strafvordering)', VU Amsterdam/Erasmus Universiteit/ Radboud Universiteit/Universiteit Utrecht van 11 september 2023, p. 60, beschikbaar

via: www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2023A02302.

26 Zie Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD TOT VASTSTELLING VAN GEHARMONISEERDE REGELS BETREFFENDE ARTIFICIËLE INTELLIGENTIE (WET OP DE ARTIFICIËLE INTELLIGENTIE) EN TOT WIJZIGING VAN BEPAALDE WETGEVINGSHANDELINGEN VAN DE UNIE, COM/2021/206 final.