

Gespreksnotitie prof. mr. Marianne F.H. Hirsch Ballin – Rondetafelgesprek over het MIT, Vaste Commissie J&V, 16 september 2021, 9.45 uur

U heeft mij gevraagd om een schriftelijke samenvatting van mijn standpunt over de toekomstige bevoegdheden van het Multidisciplinair Interventie Team (hierna: MIT) ter voorbereiding van het rondetafelgesprek met de Vaste Commissie voor Justitie en Veiligheid. In deze gespreksnotitie geef ik mijn standpunt – en daartoe is het dus ook beperkt – vanuit mijn expertise als hoogleraar Straf- en strafprocesrecht. Mijn standpunt heeft daarom betrekking op de juridische normering die nodig is gelet op de beoogde taken en bevoegdheden van het MIT.

De beoogde activiteit van het MIT is het “op basis van toegang tot en eigen verwerving van relevante gegevens [maken van] proactief hoogwaardige systeemgerichte analyses en integrale informatiebeelden over criminele systemen die een bedreiging (kunnen gaan) vormen voor de Nederlandse rechtsstaat.”¹ Daartoe dient het MIT een zelfstandige entiteit te worden met eigen bevoegdheden voor informatieverwerving en -verwerking. Blijkens de kamerbrief van 11 mei 2021² gaat het daarbij niet alleen om informatie verkregen door opsporingsdiensten, maar ook om relevante gegevens waarover andere overheidsorganisaties bij hun taakuitoefening de beschikking hebben gekregen.

De activiteiten waarmee het MIT zich moet gaan bezighouden, raken aan verschillende juridische kaders, terwijl tot nu toe geen van die kaders ervoor is ingericht. Waar het gaat om de bestrijding van criminaliteit zijn dit het Wetboek van Strafvordering en voor de politietaak buiten de context van de opsporing de Politiewet 2012 en de Wet politiegegevens. Andere actoren die interventies kunnen plegen in de strijd tegen ondermijnende criminaliteit, zoals Belastingdienst, douane, DNB, gemeentes, opereren binnen het bestuursrechtelijke kader met toezichtsbevoegdheden op grond van de Algemene wet bestuursrecht of bijzondere wetten.³ Denkbaar is ook dat het werkterrein van het MIT het terrein van de inlichtingen- en veiligheidsdiensten zal raken (en aldus de voorschriften van de Wet op de inlichtingen- en veiligheidsdiensten 2017). Zelfstandige *informatieverwerving* en *informatieverwerking* door het MIT, met als doel datakoppeling en -analyse ten behoeve van interventies door andere organisaties (in de regel strafrechtelijke opsporing of bestuursrechtelijk toezicht of handhaving), zal slechts kunnen plaatsvinden indien die bevoegdheden worden voorzien van een voldoende wettelijke grondslag.

Voorzien in een voldoende wettelijke grondslag is geen gemakkelijke opdracht. In de traditionele kaders van strafvordering, bestuurlijke controle en toezicht (inclusief de privacyrechtelijke wetgeving zoals de Wet politiegegevens) past dit niet zonder meer. Preventie met behulp van datakoppeling en data-analyses, met als doel grip krijgen op criminele structuren, is een activiteit die plaatsheeft zonder dat (al) sprake is van een op het individu toegesneden verdenking (of aanwijzing) van een strafbaar feit. Het Wetboek van

¹ *Kamerstukken II 2020/21*, 29911 nr. 308.

² *Ibid.*

³ Het MIT dient zich te gaan richten op criminele systemen die een bedreiging (kunnen gaan) vormen voor de Nederlandse rechtsstaat. In de toekomst zouden dergelijke systemen ook beschouwd (kunnen gaan) worden als een bedreiging voor de nationale veiligheid en aldus in het werkterrein van de inlichtingen- en veiligheidsdiensten gaan vallen.

Strafvordering regelt dergelijke activiteiten niet. Een grondslag voor preventief onderzoek kan wellicht worden gezocht in de algemene politietaak als omschreven in artikel 3 Politiewet 2012 of in de Wet politiegegevens. Daarin zijn immers bepalingen opgenomen die verwerkingen van gegevens door de politie regelen. Ook deze bepalingen zijn echter te algemeen en onvoldoende toegesneden op geavanceerde datakoppeling en data-analyse vanuit een preventief perspectief.⁴ Kortom: de beoogde activiteiten van het MIT hebben een karakter dat niet past binnen de huidige kaders voor opsporing en handhaving, reeds omdat die kaders stammen uit een tijd waarin men de huidige technologische mogelijkheden niet heeft voorzien.

De beoogde wettelijke bevoegdheden van het MIT zijn dan ook nieuw en *aanvullend* op de bestaande mogelijkheden.⁵ Voorzien in dergelijke bevoegdheden is tegelijkertijd niet zonder risico's. Preventieve dataverwerving en preventieve datakoppeling en -analyse zijn activiteiten die (potentieel) tot een vergaande ingreep in de persoonlijke levenssfeer leiden. Het EHRM heeft in enkele recente zaken inzake vergaring van bulkdata (door inlichtingen- en veiligheidsdiensten) duidelijk gemaakt dat dergelijke bevoegdheden de meest precieze regulering behoeven en moeten zijn voorzien van '*end-to-end-safeguards*'.⁶

Juist om die reden is van belang dat we de activiteiten van het MIT niet gaan proberen in te passen in de bestaande kaders. Die volstaan niet omdat ze te veel zijn toegespitst op op het individu gerichte voorwaarden in relatie tot strafbaar gedrag en onvoldoende normering inhouden voor datakoppeling en -analyse ná vergaring. (Dat geldt in het bijzonder voor het strafvorderlijk kader, maar ook voor de normering van bestuursrechtelijk toezicht/controletaken). Ze volstaan bovendien niet omdat ze te weinig rekening houden met de omstandigheid dat de informatieverwerving, -koppeling en -analyse gericht is op het zicht krijgen op strafbare feiten waardoor strafvorderlijke waarborgen ontbreken (dat geldt ook voor het Wetsvoorstel Gegevensverwerking door samenwerkingsverbanden).⁷

Kortom: de beoogde bevoegdheden van het MIT bevinden zich uit oogpunt van normering in nieuw land, op het grensvlak van strafvorderlijke opsporing, bestuursrechtelijke handhaving en privacyrecht (dat in belangrijke mate wordt gevormd door het EVRM en het EU-recht⁸). Als proactieve dataverwerving, -koppeling en -analyse inderdaad een onmisbaar instrument

⁴ Waarom deze wettelijke grondslagen ongeschikt zijn voor preventieve datakoppeling wordt toegelicht in L. Stevens, M.F.H. Hirsch Ballin, M. Galič e.a., 'Strafvorderlijke normering van preventief optreden door datakoppeling. Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond', *TBSH* 2021, 4.

⁵ De activiteiten lijken op de praktijk van predictive policing, maar omvatten mogelijk meer aspecten. Pilots of nieuwe projecten waarin preventieve risicoanalyses de basis vormen voor vervolgoptreden zijn tot op heden vaak weer gestaakt vanwege onduidelijkheden over de wettelijke grondslag en wegens onvoldoende privacyrechtelijke waarborgen (vgl. bijvoorbeeld het Sensing project Roermond (zie voornoemde publicatie) en SyRI).

⁶ Zie met name EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013, appl. nos. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch and others v. United Kingdom*), par. 330. Zie ook: 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 (te verschijnen september 2021).

⁷ Zie uitgebreider: L. Stevens, M.F.H. Hirsch Ballin, M. Galič e.a., 'Strafvorderlijke normering van preventief optreden door datakoppeling. Een analyse aan de hand van de casus 'Sensingproject Outlet Roermond', *TBSH* 2021, 4.

⁸ Niet alleen de AVG en de Richtlijn gegevensbescherming opsporing en vervolging 2016/680, maar ook de op handen zijnde EU regulering van gebruik van artificial intelligence (zie: COM/2021/205 final).

is om grip te krijgen op de complexe structuren van internationaal opererende criminele organisaties, is het noodzakelijk een nieuwe normeringsstructuur in te richten met elementen uit het strafprocesrecht, het bestuursrechtelijke handhavingsrecht en het privacyrecht.

Bij het inrichten van die nieuwe normeringsstructuur moet de samenhang met bestaande (uitvoerings)kaders in het oog worden gehouden, nu de 'output' van het MIT zal dienen als de basis voor interventies van bijvoorbeeld openbaar ministerie, gemeentes, belastingdienst of inlichtingen- en veiligheidsdiensten. Van belang is voorts dat wordt voorzien in gedegen toezicht, ook vooraf, en dat doel en reikwijdte van vergarings- en verwerkingsbevoegdheden voldoende zijn afgebakend. Verder moet worden beoordeeld of de rechtsbescherming zoals geregeld in de Algemene wet bestuursrecht hierover toereikend is en hoe de verhouding tot de bijzondere voorschriften in de Wet op de inlichtingen- en veiligheidsdiensten 2017 uitpakt. Daarbij speelt ook de aanwijzing van het voor beheer, verwerking en verstrekking verantwoordelijke orgaan een rol: voor de daarin te maken keuzes – zelfstandig of als onderdeel van bijvoorbeeld de politie – zal bepalend moeten zijn waar de waarborging zowel van relevante strafvorderlijke als van privacyrechtelijke beginselen met inachtneming van de fundamentele rechten het beste kan worden verzekerd, mede gelet op de relatie met het in te stellen toezicht en de rechtsbescherming.

Marianne Hirsch Ballin
12 september 2021