UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Financiële surveillance en de rol van de Financial Intelligence Unit (FIU) in Nederland

Lagerwaard, P.

DOI
10.5553/BenM/138900692022001001

Publication date
2022

Document Version
Final published version

Published in
B en M : Tijdschrift voor Beleid, Politiek en Maatschappij

Link to publication

Citation for published version (APA):
Lagerwaard, P. (2022). Financiële surveillance en de rol van de Financial Intelligence Unit (FIU) in Nederland. *B en M : Tijdschrift voor Beleid, Politiek en Maatschappij*, *49*(2), 128-153. https://doi.org/10.5553/BenM/138900692022001001

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:13 Nov 2026

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Financiële surveillance en de rol van de Financial Intelligence Unit (FIU) in Nederland

*Pieter Lagerwaard**

Inleiding: De FIU-Nederland

> 'Achter elke criminele euro zit een verhaal. Een verhaal dat niet aan een bankbiljet of girale overboeking af te lezen is maar toch om een reden bij FIU-Nederland terecht komt.' (Akse, 2019, p. 6)

Ter gelegenheid van het 25-jarig bestaan van de Nederlandse Financial Intelligence Unit (FIU) bracht de politieorganisatie een jubileumboek uit, waarin de ontstaansgeschiedenis en kerntaken van de FIU worden besproken (Akse, 2019). Het boek geeft concrete voorbeelden van de bestaansreden van de FIU, zoals toen een vrouw 100.000 euro in cash op wilde nemen om – zo waren de vermoedens – haar ex-vriend te laten vermoorden. Dit geld werd derhalve niet uitgekeerd. Een ander, meer bekend voorbeeld is de bijdrage van de FIU aan het onderzoek naar Volkert van der Graaf, de moordenaar van Pim Fortuyn. Op basis van financiële gegevens van de FIU kon de politie op de dag van de moord zijn verblijfplaats achterhalen. Volgens het jubileumboek heeft 'de informatie van gemelde transacties (…) steeds meer een eigen plek in de opsporing en vervolging verkregen. (…) Of het nu om de moord op Fortuyn ging, om een betaling van een container fruit met daar tussen partijen cocaïne, of om smeergeld zorgfraude ging, (…) gemelde transacties speelden een cruciale of ondersteunende rol in al dit soort onderzoeken' (Akse, 2019, 8).

De FIU is de afgelopen 25 jaar uitgegroeid tot de spil van financiële surveillance in Nederland. Gepaard aan de toenemende digitalisering van het betalingsverkeer, van munt- en briefgeld naar digitale transacties, is er een groeiende hoeveelheid data beschikbaar van financiële transactiegegevens, niet alleen van banken, maar ook van winkels en grote betaaldienstverleners zoals Western Union. Deze data bieden een schat aan informatie over het betalingsverkeer en het bestedingsgedrag van burgers en geven daarmee mogelijk inzicht in criminele handelingen. Commerciële bedrijven zoals banken die over de transactiegegevens beschikken, worden daarom vaak gezien als 'poortwachters' van het financiële systeem. Zij moeten volgens de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) hun klanten monitoren op ongebruikelijke, mogelijk criminele activiteiten. In Nederland hebben banken inmiddels naar schatting meer dan 12.000 medewerkers in dienst die als primaire taak hebben om klantonderzoek te verrichten, het betalingsverkeer en transactiegedrag van Nederlanders te monitoren, en ongebruikelijke transacties te melden bij de FIU.[1] De FIU is dé overheidsinstantie die alle ongebruikelijke transactiemeldingen van de meldplichtigen verzamelt, verder

* Pieter Lagerwaard is promovendus aan de Universiteit van Amsterdam (politicologie).

doi: 10.5553/BenM/138900692022001001

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

onderzoekt, en bij de bevestiging van verdacht gedrag deze informatie doorgeeft aan de relevante opsporings- en vervolgingsinstanties.

Gezien de spilpositie die de FIU bekleedt in het systeem van financiële surveillance, is het opmerkelijk hoe weinig er bekend is over het dagelijks reilen en zeilen van deze relatief nieuwe organisatie. Er is een groeiende literatuur die zich richt op het toenemende gebruik van financiële gegevens voor veiligheidsdoeleinden (Amicelle, 2017b; Boy, 2017; De Goede, 2010; Vlcek, 2007; Wesseling, 2013), de rol van banken en technologie in het bestrijden van terrorismefinanciering (Bosma, 2019), en de rechtszaken die uit deze veiligheidsinspanningen voortkomen (Anwar, 2020). Maar er is weinig bekend over de exacte rol die de FIU speelt in het bredere systeem van financiële surveillance. Er zijn noemenswaardige uitzonderingen van studies die onderzoeken hoe banken en FIU's samenwerken (Amicelle, 2017a), hoe FIU's in Europees verband samenwerken en het juridische kader waarbinnen dit gebeurt (respectievelijk Lagerwaard, 2020; Mouzakiti, 2020), en hoe FIU's op internationaal niveau intelligence uitwisselen (Amicelle & Chaudieu, 2018), maar er bestaat, naar mijn weten, geen gedetailleerde studie van de dagelijkse praktijk van een enkele FIU. Daarnaast is er in de literatuur over surveillance weinig aandacht voor deze vorm van *financiële* surveillance en met name de rol van de FIU. De FIU is zowel geen conventionele 'orwelliaanse' publieke veiligheidsdienst omdat ze gebruikmaakt van privébetalingsgegevens (Orwell, 1949), alsook geen groot privaat bedrijf zoals Google of Facebook dat zijn database inzet om gedrag te monitoren voor commerciële doeleinden, wat Zuboff onlangs 'Surveillance Capitalism' heeft genoemd (2019).

Het is belangrijk om de werking van financiële surveillance en de rol van de FIU uit te lichten, omdat de informatie die er rondgaat vaak gevoelige privéinformatie betreft die vraagstukken van privacy en proportionaliteit oproept. FIU-data bevatten niet alleen financiële informatie, maar een variëteit aan andere gegevens die de transacties contextualiseren – want een transactie *an sich* is weinig informatief. Zoals Ferrari (2020, 522) stelt: 'triangulated with other personal datapoints, [financial transactions] allow to infer information about individuals' activities, purchases and geographical movements, from which, in turn, sexual orientation, health status, religious and political beliefs and cultural preferences can be derived'. In het maatschappelijke debat ligt vaak de nadruk op het verzamelen van persoonsgegevens door private bedrijven zoals Google en Facebook (Van Dijck, 2014; Zuboff, 2019) of het gebruik van kunstmatige intelligentie (Timan & Grommé, 2020), maar de verspreiding van deze financiële informatie, waarbij transacties de basis vormen van digitale risicoprofielen van burgers, wordt doorgaans niet in verband gebracht met privacy en proportionaliteit (een uitzondering vormt het werk van Dehouck & De Goede, 2021; Mitsilegas & Vavoula, 2016; Riemslag Baas, 2021). In toenemende mate wordt deze financiële informatie toegepast door commerciële bedrijven (Westermeier, 2020), zoals zogenaamde FinTechs: bedrijven die hoofdzakelijk financiële technologieën ontwikkelen en toepassen (Hendrikse, Bassens & Van Meeteren, 2018). Maar het gebruik van deze data door *publieke* actoren zoals de FIU blijft onderbelicht. Dit verschil is belangrijk omdat, zoals Mouzakiti

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

beargumenteert (2020), FIU's onder verschillende juridische kaders kunnen vallen, zowel onder de Algemene verordening gegevensbescherming (AVG) als onder opsporingskaders zoals de Europese Police Data Protection Directive of, in Nederland, de Wet politiegegevens. Omdat data van miljoenen transacties worden verzameld, geanalyseerd, verdacht verklaard en opgeslagen in databases *zonder* kennisgeving van de personen of bedrijven die de transacties hebben verricht, is een goed begrip van de werking van financiële surveillance en de rol van de FIU belangrijk: het treft (de privacy van) eenieder met een bankrekening.

Dit artikel onderzoekt de kerntaken van de Nederlandse FIU en plaatst deze in het bredere systeem van financiële surveillance.[2] Het stelt de vraag hoe de FIU, in de praktijk, invulling geeft aan de drie kerntaken van het *verzamelen*, *analyseren* en *dissemineren* van (financiële) informatie en hoe ze opereert als cruciale spil in het systeem van financiële surveillance. De studie heeft methodologische uitdagingen, omdat bepaalde activiteiten vanwege geheimhouding niet toegankelijk zijn voor onderzoek, met name het daadwerkelijke analyseproces van de FIU. De database van de FIU is staatsgeheim geheim, wat betekent dat directe verslaggeving niet gepubliceerd mag worden. Dit artikel 'omcirkelt' deze geheimhouding door alternatieve bronnen te raadplegen die inzicht geven in de dagelijkse handelingen van de FIU (Bosma, De Goede & Pallister-Wilkins, 2019; zie ook Bellanova & Sætnan, 2019). Het artikel is geïnteresseerd in de dagelijkse praktijk, de organisatorische processen en de dilemma's en uitdagingen van de FIU, die anoniem en zonder kennisgeving van mogelijk gevoelige informatie in kaart gebracht worden. De methode van omcirkelen wordt aangevuld door documentanalyse en semigestructureerde interviews met werknemers van zowel de Nederlandse FIU als Europese FIU's, waardoor generieke bronnen empirisch gesitueerd worden.

De volgende paragraaf bespreekt de theoretische achtergrond van financiële surveillance. Vervolgens worden de methode van het 'omcirkelen' van geheimhouding en de bronnen van het artikel besproken. Het empirische gedeelte beslaat het grootste gedeelte van het artikel en bestaat uit drie paragrafen die elk een kerntaak van de FIU behandelen: het verzamelen, analyseren en dissemineren van (financiele) informatie. In de conclusie bezie ik de FIU en het systeem van financiële surveillance in een academisch en maatschappelijk kader, door aandachtspunten te formuleren die kunnen dienen als startpunt voor verder onderzoek en een breder debat over financiële surveillance en de rol van de FIU, in Nederland.

Financiële surveillance

Surveillance is een breed concept dat met verschillende nuances wordt toegepast. Misschien wel het bekendste, en meest tot de verbeelding sprekende begrip van surveillance is de orwelliaanse Big Brother: een staatsdictator die de gecentraliseerde macht aanvoert en zijn 'gedachtenpolitie' via televisieschermen minutieus het gedrag van de bevolking in de gaten laat houden (Orwell, 1949, 2). Deze klassieke interpretatie van surveillance volgt een weberiaanse invalshoek, waarin de staat en bureaucratie centraal staan (zie bijvoorbeeld Dandeker, 2007, 40). Een an-

Beleid en Maatschappij 2022 (49) 2
doi: 10.5553/BenM/138900692022001001

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

der tot de verbeelding sprekend begrip van surveillance is het foucaultiaanse Panopticum: de wachttoren in het midden van een ronde gevangenis met geblindeerde ramen waardoor de cipier niet *hoeft* te kijken, maar *mogelijk* kijkt, waardoor gevangenen gedragingen internaliseren (Foucault, 1977). Naast deze twee kernbegrippen bestaan er tal van andere invalshoeken, zoals de moderne 'fluïde' vorm van surveillance waarin macht en verantwoordelijkheden gedecentraliseerd zijn (Bauman & Lyon, 2013), of de surveillance van technologie en grote digitale datasets die 'data doubles' van personen produceren (Haggerty & Ericson, 2000). Lyon, Haggerty en Ball (2012) stellen dat 'interest in surveillance studies has mushroomed, generating considerable excitement about the potential for new ways to understand human behavior' (p. 1).

Het is opmerkelijk dat een veld zo groot als *financiële* surveillance, dat geografisch wijdverspreid is door middel van meer dan 160 nationale Financial Intelligence Units die commerciële datasets analyseren met behulp van politie- en andere overheidsgegevens, geen substantiële positie bekleedt in de studie van surveillance. Veel bestudeerde onderwerpen zijn de opkomende CCTV-camera's in het publieke domein (Armstrong & Norris, 1999) of de surveillerende rol van de informatiestaat (Weller, 2012). Maar ook minder bekende onderwerpen worden bestudeerd vanuit de surveillancelens, zoals het gebruik van smarttelefoons om gezondheid te monitoren (Lupton, 2012) of de toenemende toepassing van data van vliegtuigpassagiers, die worden ingezet voor veiligheidsdoeleinden (Bellanova, 2014; Bellanova & Duez, 2012). Financiële surveillance heeft in deze literatuur geen prominente positie, maar er zijn enkele uitzonderingen. Atia (2007) heeft in de nasleep van de aanslagen van 9/11 een toenemende financiële surveillance van islamitische groeperingen geconstateerd, Vlcek (2007, 2009) heeft in Europa geobserveerd hoe terrorismefinanciering legitimering biedt om financiële surveillance te implementeren, en Amicelle beargumenteerde in 2011 al dat we een nieuw begrip van financiële surveillance moeten ontwikkelen – een nieuwe 'politieke anatomie' – waar meerdere actoren met heterogene doelen worden inbegrepen (2011, 162; zie ook Amicelle & Favarel-Garrigues, 2012).

Gerelateerde literatuur, die meer leert over deze variëteit aan betrokken actoren, richt zich niet op surveillance, maar op de 'finance-security nexus' (Boy, Morris & Santos, 2017; De Goede, 2010; Langley, 2017; Westermeier, 2019). Deze literatuur onderzoekt de verschillende manieren waarop financiën en veiligheid vervlochten zijn, zoals het gebruik van financiële middelen in oorlogssituaties (Gilbert, 2015). In toenemende mate richt deze literatuur zich op het gebruik van financiële transacties voor veiligheidsdoeleinden (Amoore & De Goede, 2008; Boy e.a., 2017). Marieke de Goede spreekt van een 'chain of financial security', waarbij de financiële transactie-informatie door een 'keten' van actoren reist: van commerciële actoren, zoals de banken die betalingsgedrag monitoren, naar de FIU, die verdere analyse verricht en de verdachte informatie doorgeeft aan de uitvoerende instanties, naar uiteindelijk de rechtbank, waar een verdachte veroordeeld kan worden op basis van financiële intelligence. De transactie-informatie blijft niet hetzelfde terwijl deze door de keten beweegt, maar 'vertaalt' en krijgt een andere betekenis in elk profes-

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

sioneel domein (De Goede, 2017a, 29). Volgens De Goede bekleedt de FIU een centrale positie in deze keten, gepositioneerd tussen de commerciële en publieke actoren. Er is echter 'very little (…) known about how FIUs handle, share, and analyse unusual transaction reports' (p. 35; zie ook De Goede, 2017b).

Dit artikel verstaat onder het systeem van financiële surveillance een breed gedragen samenwerking van private en publieke actoren die systematisch transactie-informatie monitoren, filteren, analyseren en toepassen om het betalingsverkeer en bestedingsgedrag van burgers in kaart te brengen om criminele misdragingen op te sporen en zo mogelijk te vervolgen en bestraffen. De FIU is misschien wel de belangrijkste actor, de spil, in dit systeem omdat ze de enige actor is die puur op het kruisvlak van financiën en veiligheid opereert, met transactieonderzoek als primaire taak. De rol van spil kan vergeleken worden met een zandloper: aan de kant van de meldplichtigen zijn er 25 beroepsgroepen – niet alleen financiële – die ongebruikelijk betalingsverkeer moeten melden bij de FIU.[3] Deze actoren sturen hun informatie naar de FIU, zoals het zand van een loper vanuit een brede basis naar de kern beweegt. De FIU analyseert de meldingen, waarna ze de intelligence naar tal van politie-, justitie- en veiligheidsdiensten stuurt, zoals het zand vanaf de kern van een zandloper weer de breedte instroomt. Echter: de FIU filtert de intelligence, vult deze aan en modificeert haar, zodat de intelligence toegepast kan worden door de actoren verderop in de keten (zie bijvoorbeeld Amicelle, 2020).

Wat de FIU zo interessant maakt, is dat ze opereert in de kern van de zandloper als spil op meerdere kruisvlakken. De FIU opereert op het kruisvlak van *financiën* en de wereld van banken en economische transacties aan de ene kant, en de wereld van *veiligheid* zoals politie en justitie aan de andere kant. De FIU opereert als een spil op het kruisvlak van zowel *private* actoren (omdat ze afhankelijk is van de privétransactiegegevens) als *publieke* instanties waaraan ze de informatie door moet geven wil er iets mee gebeuren. De FIU is daarnaast zelf een kruisvlak waar *ongebruikelijke transactie-informatie* naar binnen gaat en *verdachte financiële intelligence* naar buiten. Tot slot speelt de FIU een belangrijke rol op het internationale toneel door de intelligence te delen met FIU's uit andere landen, die intensief (moeten) samenwerken om verdachte internationale geldstromen in kaart te brengen (Amicelle & Chaudieu, 2018). Het is opmerkelijk dat ondanks deze spilpositie de specifieke rol van de FIU in het bredere systeem van financiële surveillance zowel in de wetenschappelijke literatuur als in het maatschappelijke en beleidsmatige debat, sterk onderbelicht is.

Het 'omcirkelen' van geheimhouding

Om de geheime processen in de FIU te kunnen onderzoeken maak ik gebruik van de methode van het 'omcirkelen' van geheimhouding (Bosma e.a., 2019, 14). De data van de FIU, zoals de ongebruikelijke transacties, zijn op het moment dat deze in de FIU-database worden opgenomen staatsgeheim geheim. Er zijn vier categorieën gevoelige informatie bij de rijksoverheid: departementaal vertrouwelijk, staatsgeheim confidentieel, staatsgeheim geheim en staatsgeheim zeer geheim.[4]

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

De data van de FIU vallen in de derde categorie – staatsgeheim geheim –, wat betekent dat er specifieke beveiligingsmaatregelen van toepassing zijn, zoals het registreren van alle personen aan wie de informatie is uitgereikt, het ondertekenen van een geheimhoudingsverklaring en het bezitten van een Verklaring van Geen Bezwaar (VGB).[5] Deze geheimhouding is niet zonder reden. De informatie waar de FIU zich mee bezighoudt, is privacygevoelig, en het onthullen van de exacte onderzoeken van de FIU of de personen van wie de informatie bewaard wordt, zou schadelijk kunnen zijn voor opsporing en vervolging, ook omdat de personen of bedrijven wier informatie opgeslagen is hier niet van op de hoogte zijn. Met name de geheimhoudingsverklaring maakt het lastig voor onderzoekers om veiligheidsinstanties zoals de FIU te onderzoeken, want zonder toestemming is er geen mogelijkheid om de analyseprocessen te onderzoeken, maar met toestemming is het niet toegestaan om erover te publiceren.

Er is een groeiende literatuur die onderzoek doet naar geheimhouding (Birchall, 2016) en de methodologische vraagstukken die hiermee gepaard gaan (Belcher & Martin, 2019; De Goede e.a., 2019; Dijstelbloem & Pelizza, 2019). Bosma en anderen stellen dat 'we do not consider closed doors, partial visibilities and obfuscation necessarily to constitute failed research. Instead of considering what has been lost or what stays out of the picture, we ask, what does mapping the contours of secrecy and obfuscation *add* to our analysis?' (2019, 3). Geheimen hebben de allure van authenticiteit omdat ze moeilijk te controleren zijn (Jones, 2014). Dit betekent echter niet dat geheimen 'onthuld' moeten worden om iets te onderzoeken, omdat de positie en betekenis van een geheim onderzocht kunnen worden zonder de daadwerkelijke inhoud te kennen. In het geval van de FIU betreft het geheim geen ondoorgrondelijk proces, maar is de data-analyse vaak een routineus – en zelfs een beetje saai – proces. Hoewel algemene kennis van deze activiteiten belangrijk is, vormt het geheim niet een dermate onoverbrugbare kennisgeving dat die een gedetailleerde studie in de weg staat. De onderzoeksbenadering van deze paper is niet om vertrouwelijke informatie of werkwijzen bloot te leggen, maar om op een creatieve methodologische wijze het obstakel dat geheimhouding opwerpt te 'omcirkelen' en zo tóch een gedegen begrip van financiële surveillance en de rol van de FIU te krijgen. Volgens Bosma en anderen (2019) houdt omcirkelen in 'a lateral, multipronged, creative, iterative approaching of secret sites, confidential materials and classified practices. It is less focused on uncovering the kernel of the secret, than it is on analysing the mundane lifeworlds of security practices and practitioners' (p. 14).

Om de analyseprocessen van de FIU te onderzoeken heb ik de e-learningcursus *Operational Analysis* gevolgd en succesvol afgerond bij de The International Centre for Asset Recovery.[6] Deze cursus is bedoeld voor FIU-analisten en heeft onder meer als leerdoel het uitvoeren van de kerntaken, het analyseren van de risico's van Suspicious Transaction Reports (STR's), het verzamelen van informatie uit open en gesloten bronnen, en het dissemineren van bevindingen. De cursus, die voornamelijk de empirische paragraaf over het analyseren van de data onderbouwt, gaat nadrukkelijk *niet* over de analysepraktijken van FIU-Nederland. Echter, door gebruik

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

te maken van actuele informatie uit de jaarrapporten van FIU-Nederland, die publiekelijk toegankelijk zijn,[7] spits ik de generieke cursus toe op Nederland. Daarnaast is dit artikel gebaseerd op vijf semigestructureerde interviews met werknemers van FIU-Nederland en acht interviews met FIU-medewerkers van Europese FIU's. Om de anonimiteit van de respondenten te waarborgen wordt er in deze paper geen gebruik gemaakt van directe quotes of referenties. De triangulatie tussen deze drie bronnen maakt het mogelijk om op een ethische manier de geheimhouding te omcirkelen, de kerntaken van de FIU te onderzoeken, en in de conclusie vraagstukken op te werpen die – hopelijk – aanzet geven voor een breder geïnformeerd maatschappelijk en academisch debat.

In de volgende drie paragrafen worden de kerntaken van de FIU besproken, die elkaar in de praktijk deels overlappen omdat de transactie-informatie door de keten beweegt en gaandeweg modificeert en 'vertaalt' in een andere betekenis (De Goede, 2017a; zie ook Latour, 1999). De paragrafen bespreken het *verzamelen* van ongebruikelijke transacties van commerciële actoren, het *analyseren* van deze data door middel van analyse en onderzoek, en het *dissemineren* van de verdachte intelligence naar binnenlandse en buitenlandse opsporings- en vervolgingsinstanties. Elke paragraaf eindigt met de opwerping van enkele vraagstukken, die in de conclusie verder aan bod zullen komen.

Verzamelen van transactie-informatie

Het verzamelen van de transactie-informatie is het fundament op basis waarvan de FIU, maar ook het bredere systeem van financiële surveillance, opereert. Zonder deze informatie heeft de FIU geen additionele bijdrage te leveren aan het opsporings- en vervolgingsapparaat. Sinds de oprichting van het Meldpunt Ongebruikelijk Transacties (MOT), in 1994, en de officiële oprichting van FIU-Nederland, in 2008, is het aantal gemelde transacties substantieel toegenomen: van 16.215 ongebruikelijke transacties in 1995, waarvan er 2218 als verdacht werden aangemerkt, naar 722.247 in 2020, waarvan er 103.947 verdacht werden verklaard. Elke vierentwintig uur ontvangt de FIU ongeveer 1200 tot 1400 meldingen, die opgeslagen worden in een transactiedatabase met gemiddeld 1,2 tot 1,4 miljoen ongebruikelijke transacties (Akse, 2019, 5-8). Wie stuurt deze transactie-informatie naar de FIU? Op basis van welke gronden worden de transacties geselecteerd? Hoe worden ze ingediend en opgeslagen?

De FIU ontvangt transactie-informatie van zogenoemde meldplichtigen, die in de media vaak worden aangeduid als de 'poortwachters' van het financiële systeem. Deze meldplichtigen bestaan niet alleen uit banken. Vele andere beroepsgroepen die op een bepaalde manier toegang hebben tot transactiegegevens en betalingsverkeer zijn op basis van de Wwft verplicht om ongebruikelijk bestedingsgedrag en transactiepatronen van hun klanten te melden bij de FIU. Ze worden geacht een verantwoordelijkheid te dragen voor het opsporen van – niet altijd financiële – criminaliteit, zoals corruptie, drugsgerelateerde activiteiten, mensenhandel en -smokkel, fraude, zorgfraude, misbruik van virtuele assets, witwassen, terrorisme-

Beleid en Maatschappij 2022 (49) 2
doi: 10.5553/BenM/138900692022001001

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

financiering, en andere vormen van criminaliteit (FIU-Nederland, 2020, 10). Er zijn 25 beroepsgroepen meldplichtig, onder wie accountants, advocaten, beleggingsondernemers, cryptohandelaren, bemiddelaars, betaaldienstverleners, belastingadviseurs, juridisch dienstverleners, casinomedewerkers, makelaars, verkopers van luxegoederen zoals goudhandelaren, autodealers, botenverkopers en sinds kort kunsthandelaren (FIU-Nederland, 2020, 50).[8] Er kan gesteld worden dat financiële surveillance en het bestrijden van financiële criminaliteit inmiddels doordringen tot de haarvaten van de economie.

De miljoenen ongebruikelijke transacties die meldplichtigen indienen, bestaan niet alleen uit financiële gegevens, maar bevatten ook aanvullende, contextualiserende informatie. De initiële ongebruikelijke transactiemelding van de meldplichtige moet op basis van artikel 16 lid 2 Wwft de volgende gegevens bevatten:

a de identiteit van de cliënt, de identiteit van de uiteindelijk belanghebbenden (…);
b de aard en het nummer van het identiteitsbewijs van de cliënt (…);
c de aard, het tijdstip en de plaats van de transactie;
d de omvang en de bestemming en herkomst van de gelden (…);
e de omstandigheden op grond waarvan de transactie als ongebruikelijk wordt aangemerkt;
f een omschrijving van de desbetreffende zaken van grote waarde bij een transactie boven de € 10.000;
g aanvullende, bij algemene maatregel van bestuur aan te wijzen, gegevens.[9]

Met andere woorden, bij de melding van een ongebruikelijke transactie vormt de financiële transactie de basis voor een bredere context en een (digitaal) profiel van een persoon die of een bedrijf dat de transactie heeft verricht. Punten a tot en met d beslaan de algemene 'harde' gegevens, zoals de identiteit (het identiteitsbewijs) van de cliënt,[10] de aard en het tijdstip van de transactie, en de omvang. Punt g betekent dat de FIU navraag kan doen bij de meldplichtige voor aanvullende informatie. Punten e en f verdienen meer uitleg, onder meer omdat deze punten twee verschillende facetten van financiële surveillance aanstippen die essentieel zijn om het gehele proces van verzamelen, analyse en disseminatie te begrijpen.

Meldplichtigen, ook in andere landen, moeten een transactie melden op basis van *objectieve* of *subjectieve* indicatoren. Punt f is een voorbeeld van een objectieve indicator. Deze omschrijft dat elke transactie met een grotere waarde dan € 10.000 onherroepelijk onderzocht moet worden. In het geval van bijvoorbeeld banken *moeten* bepaalde transacties, zoals een cashstorting van deze grootte, gemeld worden.[11] Automatisch, wanneer de 'drempel' omlaag of omhoog wordt bijgesteld, veroorzaakt die een stijging of daling van het aantal ongebruikelijke transactiemeldingen bij de FIU. Een andere objectieve indicator is de bepaling van risicolanden, zoals aangemerkt door de Europese Commissie[12] of de Financial Action Task Force,[13] waardoor *alle* transacties die plaatsvinden met deze landen als ongebruikelijk worden gekenmerkt en gemeld moeten worden bij de FIU. De objectiviteit van objectieve indicatoren zit niet zozeer in de indicator zelf – deze zijn gebaseerd op be-

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

paalde assumpties –, maar op het feit dat die 'objectief' te implementeren zijn in de vaak automatische monitoringssystemen.

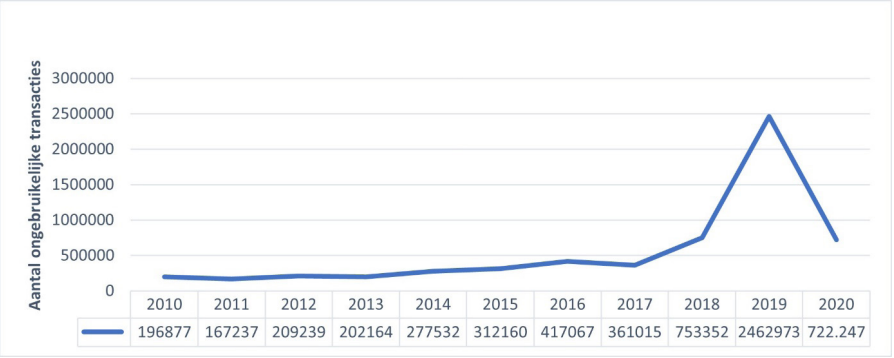
De subjectieve indicator vraagt een meldplichtige op basis van persoonlijke, normatieve vermoedens betalingsgedrag van een klant als een risico aan te merken. Punt e is hier een voorbeeld van, omdat het de meldplichtige voorschrijft de omstandigheden te beschrijven die de transactie ongebruikelijk maken. De Belastingdienst interpreteert dit punt als 'om welke reden u de transactie ongebruikelijk vindt'.[14] Waar de FIU voor banken vijf objectieve indicatoren voorschrijft, is er in het geval van de subjectieve indicator één omschrijving: 'Een transactie waarbij de instelling aanleiding heeft om te veronderstellen dat deze verband kan houden met witwassen of financieren van terrorisme.'[15] Deze subjectieve indicator is aan interpretatie onderhevig en doet een beroep op het inschattingsvermogen van de melder om (financiële) criminaliteit te herkennen. Toezichthouders voor bepaalde sectoren geven richtlijnen voor de subjectieve indicatoren, zoals de Autoriteit Financiële Markten (AFM, 2020) en De Nederlandsche Bank (DNB, 2020), maar deze richtlijnen zijn geen beleidsregels en niet juridisch bindend. Zodoende vormen de normatieve vermoedens van de vele commerciële actoren voor een belangrijk deel de 'frontlinie' die de informatie aanleveren op basis waarvan het bredere systeem van financiële surveillance en de bestrijding van financiële criminaliteit rust (De Goede, 2017a).

Het aantal gemelde ongebruikelijke transacties is het afgelopen decennium sterk gestegen, zoals te zien is in figuur 1.[16] Meldplichtigen dienen hun melding in via een meldformulier of een XML-Meldrapport.[17] Het meldformulier wordt vaak gebruikt door kleine melders van bijvoorbeeld luxegoederen, die weinig meldingen doen (FIU-Nederland, z.j.). De XML-Meldrapporten worden gebruikt door grote melders zoals banken, die hun meldsystemen automatiseren door de XML – een gestructureerde opmaaktaal – af te stemmen op de XML van de FIU. Het verschilt per meldgroep hoeveel capaciteit melders investeren en hoeveel meldingen zij indienen bij de FIU. Zo meldden in 2020 casino's 3.764 en banken 245.148 ongebruikelijke transacties. Een belangrijke kanttekening bij figuur 1 en deze cijfers is dat de substantiële groei in 2019 voornamelijk voortkomt uit een herinterpretatie van de risicolanden. Deze objectieve indicator was verantwoordelijk voor maar liefst 1.921.737 ongebruikelijke transactiemeldingen in 2019 (FIU-Nederland, 2020, 31). Om dit soort meldingen te drukken is deze objectieve indicator in 2020 veranderd naar een subjectieve indicator, waardoor de meldplichtigen nu zelf moeten bepalen wat een risicoland is (FIU-Nederland, 2020). Het aantal meldingen reflecteert zodoende niet zozeer een daadwerkelijke toename van ongebruikelijk financieel gedrag in de samenleving, maar toont dat de kaders en naleving van de indicatoren in grote mate de toe- of afname van het aantal ongebruikelijke transactiemeldingen bepalen.

Beleid en Maatschappij 2022 (49) 2
doi: 10.5553/BenM/138900692022001001

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Figuur 1 ***Longitudinaal overzicht van het aantal ongebruikelijke transacties van FIU-Nederland***



Met het oog op de enorme aantallen ongebruikelijke transacties die de FIU ontvangt, ingestuurd door 25 meldgroepen waarvan alleen al het aantal bankmedewerkers dat betrokken is meer dan 12.000 personen betreft,[18] zou een groot personeelsbestand bij de FIU verwacht worden. Echter, de FIU is een relatief kleine organisatie met in 2020 een bezettingskracht van 76 medewerkers (FIU-Nederland, 2021, 16). Ook de financiële slagkracht is in vergelijking met banken relatief klein. De grote systeembanken in Nederland hebben de afgelopen jaren miljarden geïnvesteerd; alleen al ABN Amro heeft de afgelopen drie jaar 1 miljard (duizend miljoen) geïnvesteerd en investeert nog een miljard de komende twee jaar.[19] De FIU heeft daarentegen een jaarlijks budget van 9 miljoen euro (FIU-Nederland, 2021). Deze opmerkelijke verhoudingen roepen vragen op van proportionaliteit – staat de inzet van de meldplichtigen in verhouding tot de slagkracht van de FIU –, maar ze stippen voor de FIU bovenal een praktisch dilemma aan. Gezien de verhouding tussen de miljoenen gemelde ongebruikelijke transacties en de beperkte (financiële) capaciteit van de FIU lijkt de taak van de FIU overweldigend groot. Hoe analyseert FIU-Nederland de miljoenen ongebruikelijke transacties die dagelijks bij duizenden worden gemeld?

Analyseren van de data

> 'De database met ongebruikelijke transacties van de FIU-Nederland zit vol met transacties die kunnen duiden op witwassen of andere vormen van criminaliteit. Het is met de huidige capaciteit van de FIU-Nederland, maar ook die van opsporingsautoriteiten, niet mogelijk en overigens ook niet wenselijk alle transacties aan een even diepgaand onderzoek te onderwerpen. De FIU-Nederland heeft een model van strategische sturing en tactische selectie ontwikkeld waardoor zoveel mogelijk de juiste zaken kunnen worden onderzocht die bovendien aansluiten bij de prioriteiten van de afnemende opsporingspartners.' (FIU-Nederland, 2020, p. 59)

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Deze paragraaf bespreekt het proces vanaf het moment dat de ongebruikelijke transactie-informatie gemeld wordt, tot de verdachte intelligence de FIU verlaat. Dit proces is nadrukkelijk niet lineair – de melding wordt aangemeld, onderzocht, wel of niet verdacht verklaard, en doorgestuurd – maar *bronmatig*, waarbij de gehele database met ongebruikelijke transacties, ook wel de 'buffer' tussen melder en opsporing genoemd (Akse, 2019, 38; FIU-Nederland, 2020, 55), de basis vormt. De database met ongebruikelijke transacties (met 1,2 tot 1,4 miljoen meldingen) wordt elke dag aangevuld met nieuwe meldingen, die voor vijf jaar worden opgeslagen.[20] Deze database is daardoor niet zozeer een statische opslagplek waar informatie bewaard wordt en digitaal verstoft tot het vernietigd wordt, maar een actieve bron van informatie die continu verandert. Gezien de capaciteitsverhouding tussen melders en FIU is deze bronmatige aanpak essentieel, omdat het mogelijk maakt niet alle gemelde transacties aan vervolgonderzoek te onderwerpen, maar (routineus) zoekopdrachten van de *gehele* database uit te voeren op basis van nieuwe (externe) onderzoeksgegevens en -verzoeken. Op basis van welke gronden wordt een ongebruikelijke transactie verdacht verklaard? Wat voor analyseonderzoek verricht de FIU zelf? Hoe wordt transactie-informatie omgezet naar financiële intelligence? Deze paragraaf kijkt eerst naar hoe een ongebruikelijke transactie verdacht verklaard kan worden, waarna met behulp van de cursus *Operational Analysis* de analysemethoden van de FIU beschreven worden.

Verdachtverklaring

Typerend voor het Nederlandse systeem van financiële surveillance is de tweedeling tussen *ongebruikelijke* en *verdachte* transacties, waarbij de gemelde transactie in eerste instantie ongebruikelijk is en pas na analyse van de FIU verdacht wordt verklaard. De methoden om verdachte transacties uit de database van ongebruikelijke transacties te filteren zijn grofweg in te delen in twee groepen: de (semi)geautomatiseerde methoden – vaak *analyse* genoemd – en de handmatige methoden – vaak *onderzoek* genoemd.

De (semi)automatische methoden maken een koppeling tussen de database met ongebruikelijke transacties en externe informatiebronnen, zoals (sanctie)lijsten, databases en andere gegevensbestanden. De belangrijkste nationale database waarmee een koppeling wordt gemaakt is de Verwijzingsindex Recherche Onderzoeken en Subjecten, kortweg de VROS, een databestand van de Nationale Politie waarin 'CIE-subjecten [Criminele Inlichtingen Dienst] staan en subjecten die in onderzoek zijn bij de recherche' (KLPD, 2008, 174; zie ook FIU-Nederland, 2019, 23).[21] In 2020 zijn 42.367 transacties verdacht verklaard doordat de FIU-database matchte met VROS, ruim een derde van de totale verdachte transacties in dat jaar (FIU-Nederland, 2021, 10). Daarnaast wordt de database periodiek vergeleken met nationale bestanden van het Bureau Ontnemingen Openbaar Ministerie (BOOM) (KLPD, 2008, 174), het Centraal Justitieel Incassobureau (CJIB) (FIU-Nederland, 2020, 38) en de Nationale Sanctielijst Terrorisme (FIU-Nederland, 2020, 42). Ook buitenlandse nationale sanctielijsten en internationale lijsten zoals die van de Europese Commissie worden vergeleken (FIU-Nederland, 2020), en de database wordt (indirect en anoniem) Europees beschikbaar gesteld aan de FIU.net, het sys-

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

teem waarmee Europese FIU's data uitwisselen.[22] Deze veelvoud aan lijsten, databases en koppelingen met andere gegevensbestanden zijn (semi)automatisch omdat de informatiebronnen verdachte transacties automatisch opsporen *vanuit* de database, zonder dat er specifieke zoekacties uitgevoerd hoeven te worden.

Figuur 2 LOvJ-verzoeken per opsporings- of vervolgingsinstantie in 2020 (FIU-Nederland, 2021, 35)

Nationale Politie		Andere opsporingsdiensten	
politie eenheid - Zeeland-West-Brabant	107	FIOD	210
politie eenheid - Midden-Nederland	106	KMAR	189
politie eenheid - Rotterdam	78	ISZW	20
politie eenheid - Landelijke Eenheid	75	Arrondissementsparket	15
politie eenheid - Amsterdam	68	KMAR Schiphol	3
politie eenheid - Oost Nederland	60	Functioneel Parket	18
politie eenheid - Oost-Brabant	56	Rijksrecherche	12
politie eenheid - Den Haag	52	Sociale Recherche	13
politie eenheid - Noord-Nederland	37	NVWA-OID	13
politie eenheid - Limburg	38	ILT-IOD	6
politie eenheid - Noord Holland	34	Landelijk Parket	2
		Recherche Samenwerkingsteam	1
Subtotaal Nationale Politie	711	Subtotaal andere diensten	502

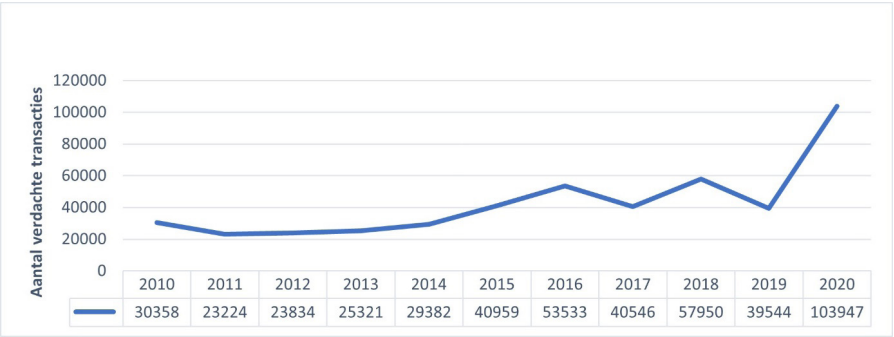
De handmatige methoden behoeven daarentegen input van *buitenaf* door gericht te zoeken naar informatie in de database. Deze verzoeken komen voornamelijk binnen via de speciaal met deze taak belaste landelijke officier van justitie (LOvJ), die als tussenpersoon voor opsporings- en vervolgingsinstanties informatieverzoeken indient, waarop de FIU de database raadpleegt, de gevonden ongebruikelijke transactie-informatie verdacht verklaart en – mogelijk met nog aanvullend onderzoek – weer terugkoppelt (Audit Magazine, 2019, 21).[23] In 2020 heeft de FIU 1213 LOvJ-verzoeken ontvangen van 23 verschillende organisaties (zie figuur 2). Een andere belangrijke handmatige methode betreft de informatie-uitwisseling met buitenlandse FIU's. De LOvJ kan de Nederlandse FIU verzoeken om informatie op te vragen bij een buitenlandse FIU, en buitenlandse FIU's kunnen verzoeken plaatsen bij FIU-Nederland (FIU-Nederland, 2020, 32). In 2020 heeft FIU-Nederland 650 informatieverzoeken ontvangen van 77 buitenlandse FIU's, en heeft ze zelf 590 verzoeken geplaatst bij 85 buitenlandse FIU's (FIU-Nederland, 2021, 7). Deze uitwisseling kan plaatsvinden via wat *diagonal cooperation* genoemd wordt, waarbij de FIU's fungeren als een postbus die informatie doorgeeft aan nationale opsporings- of vervolgingsdiensten (Amicelle & Chaudieu, 2018, 652; European Commission, 2017, 4). Omdat met name de LOvJ-verzoeken steeds complexer van aard worden, is de FIU voornemens om ook de handmatige methoden meer te (semi)automatiseren in de toekomst (FIU-Nederland, 2020, 6 en 9).

Kortom, de verdachte transacties komen voort uit het actief monitoren, filteren en doorzoeken van de gehele database van ongebruikelijke transacties. Hierdoor kan geïntensifieerd gebruik van (semi)automatische of handmatige methoden leiden

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

tot een stijging aan verdachte transacties die niet in verhouding staat tot de groei of daling van ongebruikelijke transacties. Bijvoorbeeld, in tegenstelling tot de daling aan ongebruikelijke transacties in 2020, is het aantal verdachte transacties flink toegenomen in datzelfde jaar, zoals te zien is in figuur 3.[24] De geselecteerde ongebruikelijke transacties worden officieel verdacht verklaard door het hoofd van de FIU (FIU-Nederland, 2020, 54), waarna de meldplichtige een automatische 'ontvangstbevestiging' ontvangt dat de ongebruikelijk transactie verdacht verklaard is. De persoon die of het bedrijf dat de transactie heeft verricht, wordt niet op de hoogte gesteld.[25]

Figuur 3 ***Longitudinaal overzicht van het aantal verdachte transacties van FIU-Nederland***



Het analyseproces

De Nederlandse FIU maakt de verdachte transacties breed beschikbaar voor opsporingsdiensten – waarover meer in de volgende paragraaf –, maar verricht ook eigen, aanvullende analyse. De verdachte transacties die onderling verband houden, worden samengevoegd in dossiers. De 103.947 verdachte transacties in 2020 werden samengevoegd in 19.114 dossiers (FIU-Nederland, 2021, 7), ongeveer vijf transacties per dossier. In de praktijk hangt de grootte van een dossier af van de problematiek, de onderzoekscapaciteit en het belang van de opsporingsactoren verder in de keten, en kan een dossier één, maar ook duizenden transacties bevatten (FIU-Nederland, 2021, 10). Vanwege de beperkte onderzoekscapaciteit van de FIU selecteert zij ieder jaar actuele thema's, zoals in 2019 mensenhandel, handel in drugs en 'zicht op zorgfraude' (FIU-Nederland, 2020, 33-35). De FIU heeft een bestuurlijk orgaan dat de beleidsprioriteiten bepaalt, genaamd het strategisch besturingsoverleg; en een orgaan waar voorstellen voor onderzoeken ingediend kunnen worden, genaamd het tactisch selectieoverleg, dat een voorstel beoordeelt en de benodigde capaciteit bepaalt (FIU-Nederland, 2020, 60).

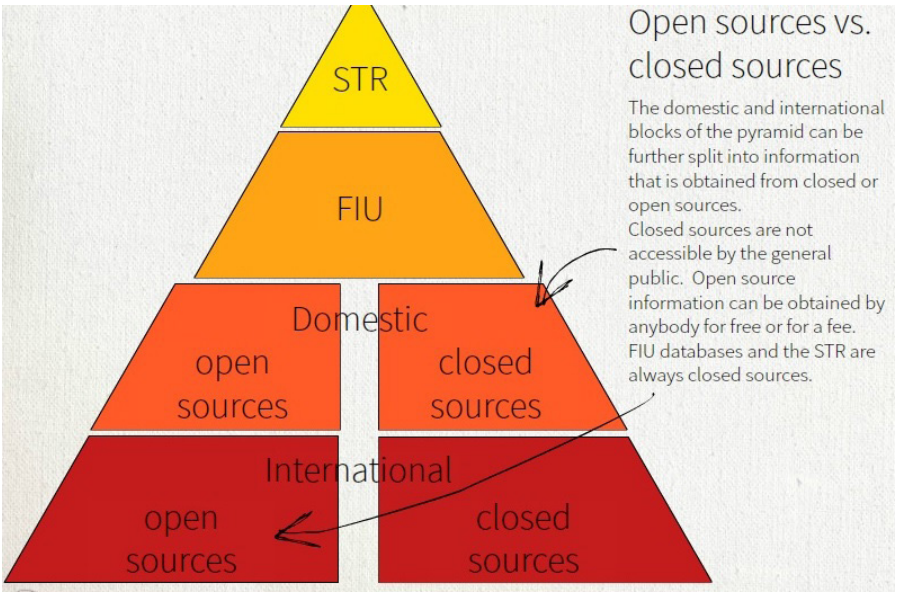
Volgens de cursus *Operational Analysis* bestaat een FIU-analyse uit een 'intelligence cycle', die zeven stappen beslaat: plannen, collecteren, evalueren, sorteren, analyseren, rapporteren en dissemineren.[26] De eerste stap, het plannen, betreft de selectie van verdachte transacties die verder onderzocht worden, wat het tactisch selec-

doi: 10.5553/BenM/138900692022001001

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

tieoverleg in het geval van FIU-Nederland grotendeels bepaalt. De tweede stap, het collecteren, concentreert zich op het verzamelen van additionele informatie. De cursus benadrukt dat deze informatie afhangt van de onderzoeksmogelijkheden die een FIU (juridisch) heeft, en tot welke bronnen zij toegang heeft. Bronnenverzameling volgt verschillende stappen die gevisualiseerd kunnen worden in een piramide (zie figuur 4), en begint bij de informatie die een meldplichtige heeft ingediend. Vervolgens raadpleegt de FIU de eigen informatie over een bepaald dossier, bijvoorbeeld op basis van onderzoekservaring en -resultaten uit het verleden. In het geval van FIU-Nederland resulteren bijvoorbeeld de geselecteerde thema's die het strategisch besturingsoverleg bepaald heeft, tot kennis- en gegevensaccumulatie.

Figuur 4 ***Bronnenverzameling van open en gesloten bronnen (Basel Institute on Governance, 2017)***



De fundamenten van de piramide bestaan uit nationale en internationale open en gesloten bronnen. De FIU-Nederland raadpleegt meerdere *gesloten* nationale bronnen, zoals de gegevens van de infobox Crimineel en Onverklaarbaar Vermogen (FIU-Nederland, 2020, 33), belastinggegevens (die opgevraagd kunnen worden) (idem, 59), en de politiesystemen waarop zij is aangesloten. Internationale gesloten bronnen komen – volgens de cursus – voort uit samenwerking met buitenlandse organisaties zoals Europol, Interpol of buitenlandse FIU's. Voornamelijk FIU's hebbenzich in de internationale samenwerking toegelegd op het zo vrijuit mogelijk delen van intelligence, inclusief de eigen gesloten bronnen (Egmont Group, 2013, 2017). Bij *open* bronnen kan er gedacht worden aan bronnen zoals het handelsregister van de Kamer van Koophandel, maar ook aan de verscheidenheid aan informatie die het internet biedt: Google, jaarverslagen van organisaties, bedrijfsweb-

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

sites, (journalistieke) programma's, wetenschappelijk onderzoek en sociale media zoals Facebook, Twitter en Instagram. FIU-Nederland maakt gebruik van *Open Source Intelligence* en heeft in 2019 speciale software ontwikkeld om 'open bronnen beter beschikbaar te maken en onderzoekers hiervoor gericht op te leiden' (FIU-Nederland, 2020, 14). De derde stap van de intelligence cycle, het evalueren, bestaat uit het beoordelen van de betrouwbaarheid en validiteit van de gevonden informatie; en stap vier, het sorteren, bestaat uit het overzichtelijk ordenen ter voorbereiding van de analyse.

Stap vijf, de analyse, bestaat uit verschillende elementen: het grondig bestuderen van de bronnen, het formuleren van een hypothese, het doen van nader onderzoek en uiteindelijk het formuleren van een onderbouwend argument. Meerdere analysemethoden – volgens de cursus – bieden hierbij ondersteuning, zoals het gebruik van een *association matrix*, waarbij bronnen verbonden worden en hun samenhang wordt bepaald, of een *link chart*, waarbij informatie en de samenhang visueel worden uitgetekend. Ook FIU-Nederland werkt met verschillende analysemethoden. Zo schrijft FIU-Nederland (2020) dat het 'met een hoogwaardig rapportage- en analysetool' gerichte rapportages en analyses maakt, waarmee 'de FIU-Nederland tracht door middel van kwalitatief onderzoek zogeheten *red flags* te identificeren waarmee juist die transacties uit de database kunnen worden gefilterd die te linken zijn aan een bepaalde criminaliteitsvorm' (p. 59). Uit de casuïstiek die FIU-Nederland vrijgeeft, kan worden opgemaakt dat er verschillende analysemethoden gebruikt worden. Zo heeft de FIU 'netwerkanalyse' toegepast voor een onderzoek naar grensoverschrijdende geldstromen (FIU-Nederland, 2020, 17), 'transactieanalyses' verricht naar criminele organisaties (Akse, 2019, 73), en zijn er 'financiële profielen' van bijvoorbeeld mensenhandel (Akse, 2019, 60), illegale wisselpraktijken (FIU-Nederland, 2020, 27) of terrorismefinanciering (FIU-Nederland, 2020, 43).

Volgens de cursus vindt er in het analysetraject een transformatie plaats van simpele informatie naar intelligence. Informatie 'is raw data. It is knowledge communicated or received concerning some fact or circumstance' (Basel Institute on Governance, 2017). Intelligence bestaat daarentegen uit de gevolgtrekking van deze informatie, aangevuld door analyse en argumenten die betekenis geven aan de informatie. De cursus definieert intelligence als een 'value-added product derived from the collection and processing of all relevant information relating to the end user's needs, which is immediately or potentially significant to the end user's decision-making process' (Basel Institute on Governance, 2017). FIU-Nederland is niet simpelweg een doorgeefluik van informatie van private partijen naar publieke instanties, maar beïnvloedt en medieert bepaalde informatie, analyseert, filtert, en onderzoekt transacties, voorziet ze van meer informatie, combineert ze, vormt argumenten, en voegt de resultaten samen in dossiers om door te sturen als intelligence. Stappen zes en zeven van de intelligence cycle richten zich respectievelijk op het rapporteren en dissemineren van financiële intelligence, het onderwerp van de volgende paragraaf.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

De bronmatige benadering, aangevuld met de eigen analyse, biedt een antwoord op de ongelijke verhouding tussen de miljoenen ongebruikelijke transacties van de meldplichtigen, en de gelimiteerde capaciteit van de FIU om deze te onderzoeken. De termijn van vijf jaar is belangrijk, omdat de bronmatige aanpak niet functioneert wanneer de data bijvoorbeeld een maand worden opgeslagen of direct vernietigd zouden worden als ze niet toepasbaar blijken. Maar de bronmatige benadering roept wederom enkele vraagstukken op omtrent privacy en proportionaliteit. Omdat ongebruikelijke transacties geselecteerd worden door commerciële actoren, zonder tussenkomst van bijvoorbeeld de officier van justitie of rechter-commissaris, is dit feitelijk een grootschalige database met informatie over burgers die niet officieel verdacht zijn – een database van 'niet-verdachten'. Personen of bedrijven waarvan de – niet alleen financiële – informatie afkomstig is, worden niet op de hoogte gesteld dat hun gegevens in de database opgenomen zijn. Daarnaast specificeren de Wwft en de FIU geen aanvraagmogelijkheden om te informeren of persoonlijke gegevens in deze database opgeslagen zijn. Door informatie van miljoenen privétransacties van niet-verdachten vijf jaar te bewaren dringt zich de vraag van proportionaliteit op: staat het systematisch verzamelen en opslaan van privégegevens van niet-verdachten in de juiste verhouding tot de veiligheidsopbrengsten? Deze vraagstukken worden vooral prangend wanneer de ongebruikelijke transactie-informatie wordt gekopieerd en opgeslagen in de speciale database voor alleen *verdachte* transacties – die actief verspreid wordt onder tal van opsporings- en vervolgingsinstanties.

Dissemineren van intelligence

> 'De grootste afnemers van de FIU-informatie zijn de opsporingsdiensten van de Nationale Politie en de FIOD. De FIU-Nederland zet in op zowel brede als gerichte verspreiding van FIU-informatie via een politie brede applicatie waar vrijwel de gehele politie toegang tot heeft. Gerichte verspreiding doet de FIU-Nederland door afspraken te maken met de afnemers van de informatie.' (FIU-Nederland, 2020, p. 59)

De derde empirische paragraaf onderzoekt, tot slot, hoe de FIU-Nederland financiele intelligence aan de man brengt. De FIU kan eigenstandig geen actie ondernemen op basis van intelligence, omdat de unit geen bevoegdheden heeft om bijvoorbeeld tot arrestatie of vervolging over te gaan. De FIU is de spil in financiële surveillance die opereert op verschillende kruisvlakken, die een brug dient te slaan tussen melders en opsporing, maar zelf geen politionele bevoegdheden heeft. Deze spilpositie is mogelijk door de bijzondere institutionele inbedding: aan de ene kant kunnen meldplichtigen hun ongebruikelijke transacties melden – zonder dat deze direct bij de politie worden ingediend –, terwijl aan de andere kant de FIU is ingebed bij de politie. De Nederlandse FIU is een zogenoemde 'hybride FIU' die is ondergebracht bij de politie, maar onder de verantwoordelijkheid staat van de minister van Justitie en Veiligheid (Akse, 2019, 38). In de Wwft – en met name artikelen 12, 13 en 14, die respectievelijk de institutionele inbedding, de kerntaken en ver-

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

antwoordlijkheden, en de juridische inkadering uiteenzetten – komt de hybride positie duidelijk naar voren: de minister van Justitie en Veiligheid heeft het algemene beheer onder zijn verantwoordelijkheid, de minister van Financiën is verantwoordelijk voor de begroting, en het hoofd van de FIU – zeg maar de directeur – wordt in overeenstemming door beide ministers benoemd. De FIU is een zelfstandig orgaan,[27] maar ze is organisatorisch ondergebracht bij de politie (Akse, 2019, 44; FIU-Nederland, 2020, 54) en verhoudt zich tot de Wet politiegegevens. Hoewel de FIU geen politie-instantie *pur sang* is, heeft zij daarom wel toegang tot de politiesystemen en netwerken en kan zij intelligence via deze wijzen verspreiden (Akse, 2019, 35 en 38). Op welke manieren en aan welke actoren maakt de FIU de database van verdachte transacties beschikbaar? Hoe draagt de FIU actief bij aan opsporings- en vervolgingsinitiatieven? Hoe wordt de informatie uiteindelijk ingezet verder in de keten?

Er zijn twee manieren van disseminatie te onderscheiden: door het beschikbaar stellen van de database van verdachte transacties en door actief samen te werken met publieke instanties die geïnteresseerd zijn in financiële intelligence. De toepassing van de database van *verdachte* transacties volgt opnieuw geen lineair proces – de intelligence wordt verstuurd, verder onderzocht en kan resulteren in een arrest – maar is wederom bronmatig. Alle transacties die verdacht zijn verklaard komen in een aparte database. Ook de transacties die toebehoren aan dossiers die uiteindelijk als niet-verdacht zijn aangemerkt na verder onderzoek van de FIU – 1645 van de 5302 dossiers in 2019, met een onbekend aantal transacties – worden opgenomen in deze database (FIU-Nederland, 2020, 38). De verdachte transacties worden geen vijf maar tien jaar opgeslagen, waardoor de database een breder tijdsbestek beslaat dan de database met ongebruikelijke transacties, met een inhoud in 2020 van 438.240 verdachte transacties (alle verdachte transacties van de afgelopen tien jaar, zie figuur 3). Daarnaast zijn de verdachte transacties meer informatief omdat ze verbonden zijn in dossiers en mogelijk voorzien zijn van additionele intelligence uit open en gesloten bronnen.

In tegenstelling tot de database met ongebruikelijke transacties, die in het (afgeschermde) bezit is van de FIU en alleen toegankelijk is voor FIU-medewerkers, wordt de database met verdachte transacties extern beschikbaar gesteld (Akse, 2019, 38).[28] Dat gebeurt via BlueView, een politiesysteem dat in 2007 integraal in Nederland is ingevoerd en toegankelijk is voor alle opsporingsinstanties.[29] In het BlueView-systeem zijn 'alle in Nederland aangemaakte processen-verbaal van aangiften, van verhoren, ambtelijke verslagen, dossiers, rapportages en documenten over in beslag genomen goederen terug te vinden (…), zolang ze niet ouder zijn dan vijf jaar'.[30] Het BlueView-systeem is door nieuwsmedia ook wel getypeerd als een manier om criminelen te 'googelen'.[31] Door via BlueView de database van verdachte transacties beschikbaar te stellen kunnen op basis van nieuwe onderzoeks- en opsporingsfeiten 'oude' data, net als in de database van ongebruikelijke transacties, pas na vele jaren toepassing vinden. Alleen niet op kleine schaal binnen de FIU, maar op nationale schaal voor opsporingsdiensten in Nederland, zoals de politie, (bijzondere) opsporingsdiensten, inlichtingendiensten, veiligheidsdiensten, het

doi: 10.5553/BenM/138900692022001001

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Openbaar Ministerie, het functioneel parket en de tien Regionale Informatie- en Expertise Centra (RIEC's). De RIEC's maken bijvoorbeeld gebruik van de verdachte transacties om 'afpakprojecten' van criminelen te organiseren (RIEC-LIEC, 2020, 22).

De tweede manier waarop FIU-Nederland financiële intelligence dissemineert is door actief samenwerking aan te gaan met publieke organisaties, zowel *bilateraal* als *meerzijdig*. Op bilateraal niveau is er op sommige dossiers directe samenwerking, met name op dossiers die de FIU de status heeft gegeven van 'embargo verdacht'. In 2020 waren er 65 dossiers van deze soort, met een totaal van 1725 transacties (FIU-Nederland, 2021, 34), die worden 'opgenomen in opsporings-, inlichtingen-, en of veiligheidsonderzoeken die in verband met een strikte geheimhouding alleen zijn gedeeld met de in het onderzoek betrokken dienst(en)' (FIU-Nederland, 2020, 38). Daarnaast heeft de FIU enkele 'hoofdafnemers', zoals de Nationale Politie en FIOD, die niet alleen gebruikmaken van de database en LOvJ verzoeken, maar ook meer gerichte manieren van samenwerken kennen waarin de FIU 'bredere inzichten' en 'specialistische kennis' deelt, ook aan bijvoorbeeld regionale politie eenheden (Ibid., 18). De FIU kan ook samenwerken met een partner op basis van de vorm van criminaliteit, zoals in het geval van terrorisme financiering met de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst, en op het gebied van mensenhandel en zorgfraude met de Inspectie van Sociale Zaken en Werkgelegenheid (FIU-Nederland, 2020, 20), waarmee ze in 2020 aan een 'zorgfraudemonitor' heeft gewerkt (FIU-Nederland, 2020, 35).

De FIU-Nederland neemt daarnaast deel aan meerdere publiek-private of publiek-publieke samenwerkingen, waarbij een variëteit aan publieke en/of private partijen om tafel gaan om een bepaalde problematiek te bestrijden. De FIU is bijvoorbeeld onderdeel van het Financieel Expertise Centrum, een samenwerkingsverband dat de integriteit van de financiële sector wil versterken en bestaat uit de politie, de FIOD en het OM, maar ook uit de Belastingdienst en de toezichthouders De Nederlandsche Bank en Autoriteit Financiële Markten. Zonder verder in detail te treden op ieder samenwerkingsverband van de FIU, is de FIU onderdeel van de Serious Crime Taskforce, de Fintell Alliance (FIU-Nederland, 2020, 19), de Terrorismefinanciering Taskforce,[32] het Financial Intelligence Center (FIU-Nederland, 2020, 20) en de interdepartementale werkgroep bevriezingsoverleg (FIU-Nederland, 2020, 42). Op internationaal niveau maakt de FIU deel uit van het Europol Financial Intelligence Public Private Partnership, de Egmont Group of Financial Intelligence Units en het EU-FIU Platform. De FIU draagt bij aan deze samenwerkingen niet alleen vanuit de eigen expertise of de database van verdachte transacties, maar omdat het als enige toegang heeft tot de database met *ongebruikelijke* transacties. Banken kunnen bijvoorbeeld in deze samenwerkingsverbanden transacties overhandigen, waarna die door de FIU verdacht worden verklaard en zo toegankelijk worden voor opsporings- en vervolgingsdiensten in de database van verdachte transacties (FIU-Nederland, 2020, 45). Zo kunnen, in de praktijk, de drie verschillende kerntaken van de FIU samenkomen.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Ondanks deze verschillende vormen van intelligencedisseminatie is het lastig om de reikwijdte en vooral de mate van de toepassing van financiële intelligence in te schatten, omdat er – naar mijn weten – geen kwantitatieve gegevens beschikbaar zijn over hoe die uiteindelijk ingezet wordt bij opsporing en vervolging. De FIU biedt in de jaarrapporten en op de website casuïstiek aan van bijvoorbeeld Covid-19-uitkeringsfraude,[33] de aanpak van een 'malafide verhuurmakelaardij',[34] het financieren van terrorisme,[35] witwassen,[36] belastingontduiking[37] en zorgfraude,[38] waarbij de intelligence van de FIU belangrijk was. Echter, deze informatie is anekdotisch en voor zowel witwassen als terrorismefinanciering – de twee kerntaken volgens de Wwft – is de inschatting dat het uiteindelijke aantal rechtszaken dat uit financiële surveillance voortkomt uit slechts enkele tientallen bestaat. Tussen 2015 en 2020 zijn er ongeveer 20 terrorismefinancieringszaken voorgekomen,[39] maar het is onduidelijk hoeveel van deze zaken uit verdachte transacties van de FIU zijn voortgekomen. Over witwaszaken zijn geen gegevens bekend, behalve enkele reacties in de media zoals van een medewerker van het functioneel parket die in 2020 meldde dat het 'zeker om enkele tientallen onderzoeken gaat in de afgelopen paar jaar.'[40] Een belangrijke reden voor de schijnbaar geringe vervolgingsopbrengsten is dat de financiële intelligence van (lopende) onderzoeken vaak één onderdeel van een crimineel onderzoek is, misschien wel een enkele pixel. Omdat hier geen kwantitatieve gegevens over worden bijgehouden, is de concrete toepassing en meerwaarde van financiële surveillance – de stap *na* de disseminatie – moeilijk in te schatten.

De reikwijdte van disseminatie is interessant voor academisch vervolgonderzoek, maar het roept wederom maatschappelijke vraagstukken op. In tegenstelling tot de database van ongebruikelijke transacties is de database van verdachte transacties niet alleen toegankelijk voor medewerkers van de FIU. Het vraagstuk van privacy komt hier nog sterker op de voorgrond dan in het geval van de database met ongebruikelijke transacties, omdat de privé-informatie van niet-verdachten niet alleen zonder medeweten wordt opgeslagen en geanalyseerd, maar ook wordt gedeeld met tal van vervolgings- en opsporingsinstanties, zonder mogelijkheid om dit te achterhalen. Ook in dit geval is er geen tussenkomst van de officier van justitie of rechter-commissaris, wat betekent dat hoewel transacties in deze database 'verdacht' genoemd worden, in juridische zin de personen en bedrijven in de database niet verdacht zijn. Volgens richtlijnen van de Nederlandse FIU voor meldplichtigen[41] biedt de Wwft wettelijke grondslag om persoonsgegevens te verwerken zonder toestemming van de niet-verdachte, zonder dat AVG-richtlijnen worden gebroken. Echter, zoals Mouzakiti aangeeft (2020, 23), staan verschillende juridische kaders waarbinnen de FIU opereert op gespannen voet, omdat het onduidelijk blijft welke dataprotectie de financiële informatie precies geniet. Dit gegeven is met name belangrijk in de internationale context, waar de FIU in 2020 met 85 buitenlandse FIU's intelligence heeft uitgewisseld, FIU's die opereren in verschillende politieke, institutionele en rechtsstatelijke contexten. Is het wenselijk dat privé-informatie van niet-verdachten nationaal en internationaal beschikbaar wordt gesteld? Staan de onduidelijke veiligheidsopbrengsten in de bestrijding van criminaliteit in verhouding tot de impact op de persoonlijke levenssfeer?

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Conclusie

Financiële surveillance is in Nederland de afgelopen decennia uitgegroeid tot een wijdverspreid systeem dat tot in de haarvaten van de economie doordringt. In toenemende mate zijn het betalingsverkeer en het bestedingsgedrag een bron geworden voor tal van opsporings- en vervolgingsdiensten die de informatie gebruiken om crimineel gedrag te ontdekken en zo mogelijk te vervolgen. De FIU-Nederland is een cruciale spil in dit systeem, omdat deze relatief nieuwe organisatie tussen de private en publieke actoren opereert; aan de ene kant afhankelijk van commerciële data die het reservoir voor de databases vormen, en aan de andere kant afhankelijk van de publieke diensten die de intelligence inzetten. Zoals het zand naar de kern van een zandloper stroomt, ontvangt de FIU miljoenen ongebruikelijke transacties van 25 meldplichtige beroepsgroepen, die samenkomen in de beschermde, staatsgeheim geheime database van ongebruikelijke transacties. Door middel van (semi) automatische analyse en handmatig onderzoek selecteert de FIU verdachte transacties, waarna aanvullend onderzoek verricht kan worden met behulp van open en gesloten bronnen en specifieke analysemethoden. Zoals het zand vervolgens weer de breedte instroomt, verspreidt de intelligence zich naar een diverse schakering aan 'afnemers'. Dit proces gebeurt niet zonder beïnvloeding; de FIU medieert actief de transactie-informatie, waarna de intelligence in de vorm van dossiers beschikbaar gesteld wordt door de database van verdachte transacties via BlueView beschikbaar te stellen voor opsporings- en vervolgingsinstanties, maar ook door actief bilaterale relaties aan te gaan en deel te nemen aan meerzijdige samenwerkingsverbanden.

In de studie van surveillance is weinig aandacht voor deze vorm van *financiële* surveillance. Financiële surveillance is geen klassieke orwelliaanse surveillance omdat het gebaseerd is op private, commerciële data (Orwell, 1949), maar de FIU is wel een publieke instantie die de intelligence doorgeeft aan andere publieke opsporings- en vervolgingsinstanties. Financiële surveillance toont aan dat dataverzameling en monitoring niet gericht hoeven te zijn op bepaalde individuen, maar – op een vergelijkbare manier als een Panopticum (Foucault, 1977) – óók niet op iedereen in een populatie. De indicatoren sturen de dataverzameling in een bepaalde richting, als besturingsknoppen waaraan gedraaid kan worden, maar vormen geen allesomvattend 'sleepnet'. Daarnaast toont financiële surveillance aan dat monitoring kan plaatsvinden op basis van intensieve samenwerking *tussen* publieke en private partijen. Het is een 'fluïde' samenwerking in de zin dat financiële surveillance nieuwe paden verkent waarover de data door de keten van actoren reizen (Bauman & Lyon, 2013)die 'vertalen' qua betekenis (De Goede, 2017a; Latour, 1999). De FIU als juridische en operationele buffer is onmisbaar in deze 'keten' van actoren omdat zij, als spil, opereert op de kruisvlakken van financiën en veiligheid, publiek en privaat, nationaal en internationaal, en de enige instantie is die 'rauwe' transactie-informatie kan omzetten in financiële intelligence.

Door de recente transformatie van een cash- naar een (digitale) transactiesamenleving is bestedingsgedrag inzichtelijk geworden en financiële surveillance mogelijk.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Maar de maatschappelijke vraag *in hoeverre* en op welke manier deze vorm van surveillance gewenst is, krijgt vooralsnog weinig aandacht, terwijl het toch gaat om een cruciale vraag die zich met de uitbreiding van het systeem steeds verder opdringt. In hoeverre is het ethisch verantwoord dat de transactie-informatie – het digitale profiel aangevuld door intelligence – over een persoon of bedrijf verdacht wordt verklaard en zowel nationaal als internationaal gedeeld wordt, terwijl persoon noch bedrijf daarvan in kennis wordt gesteld en evenmin verdacht is in officieel juridische zin? Is de privacyinbreuk proportioneel in relatie tot de bijdrage aan de opsporing en vervolging? Welke institutionele controlemechanismen en waarborgen zijn er om deze vraagstukken te reguleren, en welke externe controle is er op de rol die de FIU zich aanmeet? Dit zijn niet alleen maatschappelijke, maar ook politieke vraagstukken die thuishoren in een beleidsmatige discussie.

Noten

1 https://nos.nl/nieuwsuur/artikel/2403990-een-miljoen-ongebruikelijke-transacties-maar-weinig-aanhoudingen, geraadpleegd op 4 december 2021.
2 Dit artikel refereert aan het Engelse *surveillance* omdat de directe Nederlandse vertaling, 'toezicht', de lading onvoldoende dekt. Toezicht vertaald eerder naar *supervision*, terwijl surveillance – van het Franse *sur* (over) en *veiller* (waken) – meer de foucaultiaanse connotatie heeft van het (be)kijken, monitoren, controleren en disciplineren (Foucault, 1977).
3 www.fiu-nederland.nl/nl/melden/ben-ik-meldplichtig, geraadpleegd op 5 mei 2021.
4 https://wetten.overheid.nl/BWBR0033507/2013-06-01, geraadpleegd op 8 juni 2021.
5 https://wetten.overheid.nl/BWBR0033507/2013-06-01, geraadpleegd op 8 juni 2021.
6 Deze cursus – gevolgd in 2017 – wordt aangeboden door de Basel Institute on Governance, https://baselgovernance.org/elearning-courses/operational-analysis-english, geraadpleegd op 28 april 2021.
7 Zie voor de jaaroverzichten www.fiu-nederland.nl/nl/over-fiu/jaaroverzichten, geraadpleegd op 14 juni 2021. Dit artikel verwijst vaak naar de rapporten uit 2020 – over de gegevens van 2019 – en uit 2021 – over de gegevens van 2020 – omdat deze de meest actuele informatie bevatten op het moment van schrijven.
8 Zie ook www.fiu-nederland.nl/nl/melden/ben-ik-meldplichtig, geraadpleegd 8 juni 2021.
9 https://wetten.overheid.nl/BWBR0024282/2020-10-15, geraadpleegd 15 april 2021.
10 Meldplichtigen zoals banken worden geacht 'Know Your Customer'-beleid te implementeren. Zij worden hierbij geacht hun klanten te identificeren, verifiëren en in het geval van entiteiten zoals bedrijven of stichtingen de 'Ultimate Beneficial Owners' vast te leggen.
11 www.fiu-nederland.nl/nl/meldergroep/8, geraadpleegd 15 april 2021.
12 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:02016R1675-20181022&from=EN, geraadpleegd 6 mei 2021.
13 www.fatf-gafi.org/countries/#high-risk, geraadpleegd 8 juni 2021; zie ook www.fiu-nederland.nl/nl/faq#n773, geraadpleegd 8 juni 2021.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

14 www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/aangifte_betalen_en_toezicht/wwft-voorkomen-van-witwassen-en-terrorismefinanciering/verplichtingen/ongebruikelijke-transactie-melden, geraadpleegd 8 juni 2021.
15 www.fiu-nederland.nl/nl/meldergroep/8, geraadpleegd 8 juni 2021.
16 Figuur gebaseerd op Lagerwaard, 2018.
17 Zie ook https://meldportaal.fiu-nederland.nl/Home, geraadpleegd 8 juni 2021.
18 https://nos.nl/nieuwsuur/artikel/2403990-een-miljoen-ongebruikelijke-transacties-maar-weinig-aanhoudingen, geraadpleegd op 4 december 2021.
19 https://fd.nl/beurs/1380823/beleggers-reageren-opgelucht-na-witwasboete-abn-amro-qjf1caxuwzt3, geraadpleegd 10 juni 2021.
20 www.fiu-nederland.nl/nl/over-fiu/organisatie, geraadpleegd 8 juni 2021.
21 Uit een Kamerstuk: 'In deze [VROS] index worden niet alleen onderzoeken met betrekking tot CID-subjecten opgenomen maar ook alle onderzoeken die langer duren dan een week en die gericht zijn op misdrijven waarvoor voorlopige hechtenis is toegelaten' (Tweede Kamer, 1998).
22 Deze database van ongebruikelijke transacties wordt anoniem vergeleken in FIU.net, en pas na nader overleg met een buitenlandse FIU en het officieel verdacht verklaren van de transactie kan de buitenlandse FIU deze informatie gebruiken.
23 Zie ook www.burojansen.nl/traa/h43.htm, geraadpleegd 8 juni 2021.
24 Figuur gebaseerd op Lagerwaard, 2018.
25 www.fiu-nederland.nl/nl/over-fiu/organisatie, geraadpleegd 8 juni 2021.
26 Deze stappen zijn vertaald uit het Engels.
27 www.fiu-nederland.nl/nl, geraadpleegd 31 januari 2022.
28 Zie ook www.fiu-nederland.nl/nl/faq, geraadpleegd 17 mei 2021.
29 www.fiu-nederland.nl/nl/over-fiu/organisatie, geraadpleegd 17 mei 2021.
30 www.agconnect.nl/artikel/politie-is-zeer-tevreden-over-blueview, geraadpleegd 17 mei 2021.
31 www.nu.nl/internet/1106457/politie-kan-criminelen-googelen.html, geraadpleegd 17 mei 2021.
32 https://zoek.officielebekendmakingen.nl/stcrt-2019-43628.html, geraadpleegd 8 juni 2021.
33 www.fiu-nederland.nl/nl/veroordeeld-voor-covid-19-uitkeringsfraude-0, geraadpleegd 18 mei 2021.
34 www.fiu-nederland.nl/nl/malafide-verhuurmakelaardij-0, geraadpleegd 18 mei 2021.
35 www.fiu-nederland.nl/nl/illegaal-bankieren-en-financieren-van-terrorisme-0, geraadpleegd 18 mei 2021.
36 www.fiu-nederland.nl/nl/veroordeeld-voor-witwassen-recordbedrag-cash-0, geraadpleegd 18 mei 2021.
37 www.fiu-nederland.nl/nl/belastingontduiking, geraadpleegd 18 mei 2021.
38 www.fiu-nederland.nl/nl/transacties-zonder-zorg, geraadpleegd 18 mei 2021.
39 Zie voor jurisprudentie https://uitspraken.rechtspraak.nl/#zoekverfijn/zt[0][zt]=financiering+van+terrorisme&zt[0][fi]=AlleVelden&zt[0][ft]=Alle+velden&so=Relevance&ps[]=ps1, geraadpleegd op 8 juni 2021.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

40 www.trouw.nl/economie/tienduizenden-witwasmeldingen-amper-strafzaken-somslijkt-het-of-het-hele-meldsysteem-voor-niets-is~b03c7f64/, geraadpleegd op 8 juni 2021.

41 www.fiu-nederland.nl/nl/faq#n1222, geraadpleegd op 4 januari 2022.

Literatuur

AFM (Autoriteit Financiële Markten) (2020). *Leidraad Wwft en Sanctiewet: Toelichting op de Wet ter voorkoming van Witwassen en Financieren van Terrorisme en de Sanctiewet 1977*.

Akse, T. (2019). *Na de Poortwachters: 25 Jaar Meldingen Ongebruikelijke Transacties*. FIU-Nederland.

Amicelle, A. (2011). Towards a 'New' Political Anatomy of Financial Surveillance. *Security Dialogue*, 42 (2): 161-178.

Amicelle, A. (2017a). Policing Through Misunderstanding: Insights from the Configuration of Financial Policing. *Crime, Law and Social Change*, 69: 207-226.

Amicelle, A. (2017b). When finance met Security: Back to the War on Drugs and the Problem of Dirty Money. *Finance and Society*, 3 (2): 106-123.

Amicelle, A. (2020). Right of Entry: The Struggle over Recognition in the World of Intelligence. *Political Anthropological Research on International Social Sciences (PARISS)*, 1 (2): 243-272.

Amicelle, A., & Chaudieu, K. (2018). In Search of Transnational Financial Intelligence: Questioning Cooperation between Financial Intelligence Units. In: C. King, C. Walker & J. Gurule (red.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*. Cham: Palgrave Macmillan.

Amicelle, A., & Favarel-Garrigues, G. (2012). Financial surveillance: Who cares? *Journal of Cultural Economy*, 5 (1): 105-124.

Amoore, L., & Goede, M. de (2008). *Risk and the War on Terror*. Londen: Routledge.

Anwar, T. (2020). Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases. *International Political Sociology*, 14 (4): 382-398.

Armstrong, G., & Norris, C. (1999). *The Maximum Surveillance Society: The Rise of CCTV*. New York: Berg Publishers.

Atia, M. (2007). In Whose Interest? Financial Surveillance and the Circuits of Exception in the War on Terror. *Environment and Planning D: Society and Space*, 25 (3): 447-475.

Audit Magazine (2019). *IIA Quality Assessment Review: Veel ervaring veel toegevoegde waarde*. Instituut van Internal Auditors Nederland (IIA Nederland)/Stichting Verenigde Operational Auditors (SVRO).

Basel Institute on Governance (2017). *E-learning Course Operational Analysis*. https://baselgovernance.org/elearning-courses/operational-analysis-english.

Bauman, Z., & Lyon, D. (2013). *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

Belcher, O., & Martin, L. (2019). Site Visits, Selective Disclosure, and Freedom of Information in Qualitative Security Research. In: M. de Goede, E. Bosma & P. Pallister-Wilkins (red.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. Londen: Routledge, 33-47.

Bellanova, R. (2014). Data Protection, With Love. *International Political Sociology*, 8 (1): 112-115.

Bellanova, R., & Duez, D. (2012). A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage. *European Foreign Affairs Review*, 17: 109-124.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Bellanova, R., & Sætnan, A.R. (2019). How to Discomfort a Worldview? In: J.P. Singh, M. Carr & R. Marlin-Bennett (red.), *Social Sciences, Surveillance Technologies, and Defamiliarization*. New York: Routledge, 29-40.

Birchall, C. (2016). Six Answers to the Question 'What is Secrecy Studies?' *Secrecy and Society*, 1 (1).

Bosma, E. (2019). Multi-sited Ethnography of Digital Security Technologies. In: M. de Goede, E. Bosma & P. Pallister-Wilkins (red.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. Londen: Routledge.

Bosma, E., Goede, M. de, & Pallister-Wilkins, P. (2019). Introduction: Navigating Secrecy in Security Research. In: M. de Goede, E. Bosma & P. Pallister-Wilkins (red.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. Londen: Routledge, 1-27.

Boy, N. (2017). Finance-security: Where to go? *Finance and Society*, 3 (2): 208-215.

Boy, N., Morris, J., & Santos, M. (2017). Introduction: Taking Stock of Security and Finance. *Finance and Society*, 3 (2): 102-105.

Dandeker, C. (2007). Surveillance: Basic Concepts and Dimensions. In: S.P. Hier & J. Greenberg (red.), *The Surveillance Studies Reader*. Berkshire: Open University press, 39-51.

Dehouck, M., & Goede, M. de (2021). *Public-Private Financial Information-Sharing Partnerships in the Fight Against Terrorism Financing*. University of Amsterdam.

Dijck, J. van (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society*, 12 (2): 197-208.

Dijstelbloem, H., & Pelizza, A. (2019). The State is the Secret: For a Relational approach to the Study of Border and Mobility Control in Europe. In: M. de Goede, E. Bosma & P. Pallister-Wilkins (red.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. Londen: Routledge, 48-62.

DNB (De Nederlandsche Bank) (2020). *Leidraad Wwft en Sw* (Versie december 2020).

Egmont Group (2013). *Egmont Group of Financial Intelligence Units Principles for Information Exchange between Financial Intelligence Units*. Egmont Group of Financial Intelligence Units.

Egmont Group (2017). *Egmont Group of Financial Intelligence Units Operational Guidance for FIU Activities and the Exchange of Information*. Egmont Group of Financial Intelligence Units.

European Commission (2017). *Commission Staff Working Document: On improving Cooperation Between EU Financial Intelligence Units*.

Ferrari, V. (2020). Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy. *European Data Protection Law Review*, 6 (4): 522-535.

FIU-Nederland (2019). *FIU-Nederland Jaaroverzicht 2018*. www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu-nederland_jaaroverzicht_2018_nl_web.pdf.

FIU-Nederland (2020). *FIU-Nederland Jaaroverzicht 2019*. www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/jaaroverzicht_2019_-_fiu_nederland.pdf.

FIU-Nederland (2021). *FIU-Nederland Jaaroverzicht 2020*. https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/5169-fiu_jaaroverzicht_2020nl_web_v3.pdf.

FIU-Nederland (z.j.). Handleiding GoAML. https://meldportaal.fiu-nederland.nl/public_documents/Handleiding%20goAML%20Nederlands%20release%204%200%20(nieuw).pdf.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Gilbert, E. (2015). Money as a 'Weapons System' and the Entrepreneurial Way of War. *Critical Military Studies*, 1 (3): 202-219.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Goede, M. de (2010). Financial Security. In: J.P. Burgess (red.), *The Routledge Handbook of New Security Studies*. New York: Routledge, 100-109.
Goede, M. de (2017a). The Chain of Security. *Review of International Studies*, 44 (1): 24-42.
Goede, M. de (2017b). Banks in the Frontline: Assembling Space/Time in Financial Warfare. In: B. Christophers, A. Leyshon & G. Mann (red.), *Money and Finance After the Crisis*. John Wiley & Sons, Ltd., 117-144.
Goede, M. de (2017c). Chains of Securitization. *Finance and Society*, 3 (2): 197-207.
Goede, M. de, Bosma, E., & Pallister-Wilkins, P. (2019). *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*. Londen: Routledge.
Haggerty, K.D., & Ericson, R.V. (2000). The Surveillant Assemblage. *British Journal of Sociology*, 51 (4): 605-622.
Hendrikse, R., Bassens, D., & Meeteren, M. van (2018). The Appleization of Finance: Charting Incumbent Finance's embrace of FinTech. *Finance and Society*, 4 (2): 159-180.
Jones, G.M. (2014). Secrecy. *Annual Review of Anthropology*, 43 (1): 53-69.
KLPD (Korps Landelijke Politiediensten) (2008). *Witwassen: Verslag van een Onderzoek voor het Nationaal Dreigingsbeeld 2008*. https://docplayer.nl/1602433-Witwassen-verslag-van-een-onderzoek-voor-het-nationaal-dreigingsbeeld-2008-klpd-dienst-ipol.html.
Lagerwaard, P. (2018). *Following Suspicious Transactions in Europe: Comparing the Operations of European Financial Intelligence Units (FIUs)* (FOLLOW Research Report). Amsterdam: Amsterdam Institute for Social Science Research (AISSR).
Lagerwaard, P. (2020). Flattening the International: Producing Financial Intelligence Through a Platform. *Critical Studies on Security*, 8 (2): 160-174.
Langley, P. (2017). Finance/security/life. *Finance and Society*, 3 (2): 173-179. https://doi.org/10.2218/finsoc.v3i2.2576.
Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge/Londen: Harvard University Press.
Lupton, D. (2012). M-health and Health Promotion: The Digital Cyborg and Surveillance Society. *Social Theory & Health*, 10 (3): 229-244.
Lyon, D., Haggerty, K.D., & Ball, K. (2012). Introduction Surveillance Studies. In: K. Ball, K.D. Haggerty & D. Lyon (red.), *Routledge Handbook of Surveillance Studies*. New York: Routledge, 1-12.
Mitsilegas, V., & Vavoula, N. (2016). The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law. *Maastricht Journal of European and Comparative Law*, 23 (2): 261-293.
Mouzakiti, F. (2020). Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive. *New Journal of European Criminal Law*, 11 (3): 351-374.
Orwell, G. (1949). *Nineteen Eighty-Four*. New York: Penguin.
RIEC-LIEC (2020). *RIEC-LIEC Jaarverslag 2019*. https://www.riec.nl/documenten/jaarverslagen/2019/06/23/riec-liec-jaarverslag-2019.
Riemslag Baas, A.M. (2021). De Bijdrage van Banken aan het Voorkomen en Bestrijden van Witwassen en Terrorismefinanciering. *Tijdschrift Financieel Recht in de Praktijk*, 1: 45-51.
Timan, T., & Grommé, F. (2020). Wat is Rechtvaardige AI? Een Kader voor het Ontwikkelen en Toepassen van Algoritmes voor Automatische Besluitvorming. *Beleid en Maatschappij*, 47 (4): 425-438.
Tweede Kamer (1998). *Uitwisseling van Recherche-informatie tussen CRI en Politieregio's*. Tweede Kamer der Staten-Generaal. https://zoek.officielebekendmakingen.nl/kst-26215-4.pdf.

Dit artikel uit Beleid en Maatschappij is gepubliceerd door Boom bestuurskunde en is bestemd voor Universiteit van Amsterdam

Vlcek, W. (2007). Surveillance to Combat Terrorist Financing in Europe: Whose Liberty, Whose Security? *European Security*, 16 (1): 99-119.

Vlcek, W. (2009). Hitting the right target: EU and Security Council pursuit of terrorist financing. *Critical Studies on Terrorism*, 2 (2): 275-291.

Weller, T. (2012). The Information State: An Historical Perspective on Surveillance. In: K. Ball, K.D. Haggerty & D. Lyon (red.), *Routledge Handbook of Surveillance Studies*. New York: Routledge, 57-63.

Wesseling, M. (2013). *The European Fight against Terrorism Financing: Professional Fields and New Governing Practices* (PhD dissertation, University of Amsterdam).

Westermeier, C. (2019). Political Security and Finance – A Post-Crisis and Post-Disciplinary Perspective. *Zeitschrift Für Politikwissenschaft*, 29 (1): 105-122.

Westermeier, C. (2020). Money is Data – the Platformization of Financial Transactions. *Information, Communication & Society*, 23 (14): 2047-2063.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Londen: Profile Books Ltd.