

Verslag Bijeenkomst 'Ethische aspecten van het gebruik van de MeV-app' – vrijdag 23 juni 2023

1. Introductie

Dit verslag is tot stand gekomen op basis van een bijeenkomst die door de Gemeente Leeuwarden is georganiseerd op vrijdag 23 juni j.l. via Teams. De sessie werd geleid door [REDACTED] en [REDACTED] van Filosofie in actie. Deelnemers aan de bijeenkomst waren diverse ambtenaren van de Gemeente Leeuwarden, als ook de manager van het Veiligheidsdomein van de Gemeente Leeuwarden.

2. Casusomschrijving

Tijdens het uitvoeren van werkzaamheden stuiten medewerkers van de gemeente soms op aanwijzingen dat er sprake is van ondermijnende activiteiten. Medewerkers kunnen hun vermoeden van zulke activiteiten melden, via telefonisch of e-mailcontact met een medewerker van Openbare Orde en Veiligheid (OOV'er). In de praktijk gebeurt het melden ook soms "aan het bureau", mondeling en voor de flexplekken lag er wel eens een briefje op een bureau. Sinds 2019 kan het maken van een melding ook via een speciale app, de Meld de Vermoeden app (MeV-app). Bij het melden via de MeV-app voert een medewerker de volgende informatie in: *categorie van signaaltipe, mate van zekerheid van de melding, adres van constatering en omschrijving van signaal* en eventueel een *foto*. Van medewerkers wordt verwacht bij invullen zorgvuldig om te gaan met privacygevoelige informatie, zoals persoonsgegevens. Overigens geldt die mate van zorgvuldigheid bij alle type meldingen, dus ook wanneer de ambtenaar geen gebruik maakt van de MeV-app.

De app is in eerste instantie geïntroduceerd om het melden te stroomlijnen. Het melden gebeurde in praktijk via veel verschillende kanalen: telefonisch, per e-mail, mondeling of een briefje op een bureau. Verschillende van deze andere manieren van melden hebben risico's voor de zorgvuldigheid van het melden en de privacy van zowel de melder als de gemelde. De Meld een Vermoeden-app wordt als veiliger beschouwd dan de alternatieven omdat de melding direct terechtkomt bij de juiste afdeling en er minder mensen toegang hebben tot de (gevoelige) informatie.

In 2019 is de app uitgerold onder medewerkers van de gemeente die een toezichthoudende rol hebben, zoals BOA's. Zij zijn getraind in de werking van de app om een vermoeden te melden. Het plan was om in 2021 de app uiteindelijk uit te rollen naar *alle medewerkers van de gemeente*. De MeV-app is dus niet in gebruik voor het melden van vermoedens door burgers, zoals bij sommige andere gemeenten.

De ethische kernvraag van de bijeenkomst is **'Wat zijn de ethische aandachtspunten bij het gebruik van de MeV-app bij het doorgeven van vermoedens van ondermijnende criminaliteit?'**

Dit vraagstuk lijkt tijdens de bespreking een tweetal ethische vraagstukken in zich te hebben:

- 1) Het *melden* op zichzelf roept vragen op (ongeacht de wijze waarop)
- 2) Het gebruik van de MeV-app roept vragen op:
 - a) Is dit een geschikt middel?
 - b) Door *wie* mag er via de app gemeld worden? De initiële groep ambtenaren (2019) of *alle* ambtenaren van de Gemeente Leeuwarden (voorstel 2021)?

In het vervolg van het verslag zal deze discussie zoveel mogelijk ontward worden langs deze twee lijnen.

3. Technische aspecten

Hoe werkt MeV-app? Wat zijn belangrijke technische aspecten? Deze vragen worden hieronder beantwoord zoals ze in de sessie zijn behandeld.

De ontwikkeling en leverancier

De MeV-app is ontwikkeld en wordt geleverd door softwareontwikkelaar Pantyr, een partij die software ontwikkelt en levert aan lokale overheden. De Gemeente Leeuwarden heeft een overeenkomst gesloten voor gebruik van deze app onder de standaardvoorwaarden van het bedrijf. De software is dus van de leverancier, de data is afkomstig van de gemeente Leeuwarden.

Op de website van 'Meld een Vermoeden' is te lezen dat de leverancier de gegevens die binnenkomen via de app verwerkt. De data wordt opgeslagen in een datacentrum van een Nederlandse hostingpartij in Amsterdam. De gemeente is verantwoordelijk voor de verwerking van de gegevens door de softwareleverancier. Verder geeft de leverancier aan dat zij op aanvraag 'derdenverklaringen van audits' beschikbaar stellen en regelmatig penetratietests laten uitvoeren door ethische hackers.

Hoe gaat het in z'n werk

De ambtenaar van de Gemeente Leeuwarden installeert de app op diens telefoon en moet verificatie plegen dat diegene werkzaam is voor de gemeente en vanwege diens rol gebruik mag maken van de app. In de sessie kwam naar voren dat het onduidelijk is of het installeren van de app beperkt is tot de werktelefoon van de gemeenteambtenaar. Het eventuele gebruik op diens privételefoon heeft mogelijke gevolgen voor de toegankelijkheid van app en hoe de ambtenaar de melding kan doen (bijv. buiten kantooruren) en of dit gewenst is.

Na installatie en verificatie kan de ambtenaar via gerichte vragen een melding maken van een mogelijk ondermijnende activiteit. Deze melding wordt doorgestuurd naar een klein team van OOV'ers, die de melding via een dashboard zien binnenkomen en handmatig elke melding beoordelen. De app werkt als een berichtensysteem. Het geeft aan de ontvanger het signaal af dat er een melding is gemaakt en wat de inhoud is van de melding. Het systeem geeft geen oordeel over de melding, het is slechts een doorgeefluik. Indien de beoordelend OOV'er meent dat de melding moet worden opgevolgd, zet diegene deze door naar een afgeschermd map op de P-schijf die alleen voor twee OOV'ers toegankelijk is. De relevante informatie van lopende casuïstiek wordt daar bewaard. Dit betreft casussen die besproken wordt of nog zullen worden aan de casustafel ondermijning.

Naast de app blijven de andere, reeds bestaande, mogelijkheden om te melden ook beschikbaar: de ambtenaar houdt dus zelf de keuze hoe die de melding wil doorgeven.

Na de bijeenkomst bleek dat de speciaal opgeleide OOV'ers wel de mogelijkheid hebben om meldingen via andere kanalen zelf alsnog in de app te registreren zodat de meldingen centraal kunnen worden verzameld.

4. Juridische aspecten en context

In de sessie zijn kort juridische kaders en context aangestipt. De focus van het gesprek lag op ethische beraadslaging. Een aantal aspecten die zijn besproken:

- Ambtseed

De ambtenaar heeft bij indiensttreding een ambtseed- of gelofte afgelegd.ⁱ In de eed staan een tweetal aspecten die bijzonder relevant zijn in deze casus:

- De ambtenaar zal “niet-integere zaken aan de orde stellen”. De vraag is op wat voor niet-integere zaken wordt gedoeld. Betekent dit dat de ambtenaar verplicht is om niet-integer gedrag binnen of ook buiten de organisatie aan de orde te stellen. De in deze casus spelende vermoedens van ondermijning gaat in principe over ‘buiten’ de organisatie.
- De ambtenaar zal diens privéactiviteiten goed scheiden van diens werk als ambtenaar. In deze casus is dit relevant wanneer de ambtenaar de app op diens privételefoon heeft geïnstalleerd en/of wanneer de werktelefoon ook buiten werktijden en in privésetting wordt gebruikt.

- Intentieverklaring Friese Norm:

In 2022 is door de Provincie, het Waterschap en 18 Friese burgemeesters, waaronder die van Leeuwarden, een intentieverklaring opgesteld over een gezamenlijke aanpak van ondermijning. Onderdeel van deze aanpak is de inrichting van processen waarbij “signalen van ondermijning zorgvuldig en eenduidig worden opgepakt”. Het hebben van een intern meldpunt voor ondermijning is hierbij een van de vereisten, evenals handelen naar privacywetgeving. De specifieke invulling van het meldpunt is aan de gemeenten zelf.

- AVG

De gemeente heeft in 2022 een Gegevensbeschermingseffectbeoordeling (GEB/DPIA) laten uitvoeren op de MeV-app om de risico's op het gebied van gegevensbescherming in kaart te brengen. Hierin werd als risico aangemerkt dat de Gemeente Leeuwarden nog geen persoon had aangewezen om de bewaartermijn te waarborgen en te zorgen dat bij verstrijken van deze termijn, de gegevens ook daadwerkelijk van de server worden verwijderd. In het verlengde hiervan werden tijdens de sessie zorgen geuit over de naleving van de bewaartermijn en het verwijderen van de data uit de MeV-app zelf. Er werd benoemd dat deze data “direct” van de app verwijderd wordt, maar er bleef enige onduidelijkheid omtrent hoe direct deze verwijdering plaatsvindt en waar de verwijdering plaatsvindt (in de app of ook op de server van de leverancier).

5. Vraagstukken

a. Context van het vraagstuk

In welke context is er gekozen voor de MeV-app als *middel* tot het uiten van vermoedens? De aanleiding was dat er via verschillende kanalen signalen van vermoedens werden (en worden) geuit. Deze vermoedens zijn niet altijd voorzien van voldoende informatie en komen niet altijd (meteen) bij de juiste persoon terecht. Het doel van het melden van een vermoeden is dat er een veronderstelling is dat dit bij zal dragen aan een veiligere samenleving en gemeente in het bijzonder. Deze veronderstelling is in de sessie ook besproken (zie hieronder). Sluit de keuze voor het middel aan bij het gestelde vraagstuk en de probleempceptie en het doel dat voor ogen is? Of, zou het ook anders kunnen? In de sessie kwamen in een gedachte-experiment verschillende alternatieven naar voren: van het melden via andere wegen en systemen, andere vormen van toezicht tot meer inzet op preventieve middelen. Deze alternatieven bleken zowel een alternatief te bieden voor het melden *an sich* alswel voor het melden via de app, met daarin nog onderscheid te maken tussen de initiële groep appgebruikers (2019) en het voorstel tot uitbreiding van deze groep (2021). In de volgende paragrafen wordt op deze twee vraagstukken ingezoomd.

b. Melden als vraagstuk

Het melden op zichzelf roept vragen op tijdens de sessie. Bij het uiten van vermoedens zouden *vooroordelen* een rol kunnen spelen. Dit staat los van *hóe* er wordt gemeld. Het melden is een manier om met vroegtijdige signalen om te gaan en daar tijdig op te interveniëren. Burgers en ondernemers ondervinden hier de gevolgen van (denk aan een inbreuk op hun levenssfeer, gevoelens van stigmatisering en discriminatie), welke bij een vals positieve melding niet moeten worden onderschat. Er zijn mogelijk alternatieven voor de aanpak van ondermijning. Daarnaast bestaan er verschillende mogelijkheden om ambtenaren te trainen op betere bewustwording van vooroordelen. Een onderzoek naar de haalbaarheid en effectiviteit van deze mogelijkheden daarvan valt buiten de scope van deze sessie en verslaglegging.

c. Wie er mag melden

In de sessie kwam naar voren dat er verschillend wordt gedacht over *wie* er zou mogen melden. In de ambtseed staat dat de ambtenaar niet-integer gedrag aan de kaak moet stellen, dit geldt dus in principe voor elke ambtenaar. Zoals hierboven gesteld is het de vraag of dit gaat om niet-integer gedrag binnen de organisatie, of ook daarbuiten. De ambtenaar moet bij het melden van een vermoeden hoe dan ook altijd een zorgvuldige afweging maken tussen het belang van het melden en het mogelijke risico en de gevolgen van een melding van vermoedens. De vermoedens zijn altijd gekleurd door de ervaring, het wereld- en mensbeeld en de kennis van de betreffende ambtenaar. Een 'getrainde' BOA heeft een kennisvoorsprong en kent beter de signalen van ondermijning. Een willekeurige andere ambtenaar is daar minder goed in thuis. Dit verschil in kennis moet worden meegenomen bij de afweging om de mogelijkheid tot melding via de MeV-app uit te breiden naar alle ambtenaren. Overigens kunnen alle ambtenaren nu al melden, alleen niet via de MeV-app. De vraag is wat het gebruik van de MeV-app daarin verandert (zie d).

Er werd in de sessie gesteld dat er een machtsongelijkheid kan ontstaan wanneer ambtenaren (of dit nu de selecte groep betreft of alle ambtenaren) *wél* kunnen melden en inwoners niet. Echter is er voor inwoners andere manieren om vermoedens van misdaad en ondermijning te melden (zoals Meld Misdaad Anoniem).

d. Melden via de MeV-app

Naast de vraag *óf* er wel vermoedens moeten worden gemeld in de aanpak van ondermijning en zo ja door wie, speelt tot slot de vraag of hiervoor de MeV-app een passend middel is. Hierbij moet wederom onderscheid gemaakt worden tussen de 2019-groep (BOA's en toezichthouders) en de uitbreiding van het gebruik door alle ambtenaren. Daarbij moet ook worden opgemerkt dat de

ambtenaar altijd een keuze heeft op welke manier die meldt, hoewel er de MeV-app als voorkeurskanaal zal worden gecommuniceerd.

Een aantal vraagstukken die besproken zijn:

- **Effectiviteit:** het is onduidelijk hoe effectief de MeV-app is in gebruik (zowel qua aantal meldingen als de kwaliteit van meldingen). Hier zijn geen cijfers over bekend.
- **Privacy:** Bij het gebruik van een digitaal middel is er altijd een risico op een datalek of hack.
- **Toegankelijkheid:** De MeV-app kan, doordat het een app is en daardoor een bepaalde afstand creëert tussen mensen – men interacteert met een systeem (i.t.t. telefonisch of mailcontact) drempelverlagend werken. Dit betekent mogelijk een toename aan kwalitatief lagere meldingen en er is risico op grote werkbelasting bij de beoordelaars. Dit risico wordt vergroot bij het verbreden van de groep van gebruikers; en tegelijkertijd is er weinig over te zeggen omdat er geen cijfers zijn over de effectiviteit van de app.
- **Stigmatisering en profilering:** Ook bij het gebruik van de MeV-app blijft het risico op stigmatisering en profilering bestaan; hierbij komt dat bij het invoeren via de app bevindingen niet direct bevraagd kunnen worden.
- **Zorgvuldigheid:** Het melden door ambtenaren via een app vraagt om begeleiding in wat er onder zorgvuldig melden wordt verstaan en hoe men dat moet doen. Er wordt een instructie gegeven over de app voor diegenen die de app in gebruik gaan nemen.

6. Kernbevindingen

Tijdens de sessie werd een onderscheid gemaakt tussen ethische vraagstukken die spelen bij het melden in het algemeen, en ethische vraagstukken die spelen bij het gebruik van de app specifiek.

Een belangrijk punt van zorg dat tijdens het gesprek meerdere malen naar boven kwam heeft te maken met risico's van het uitrollen van de app onder alle ambtenaren. Momenteel wordt de app gebruikt door ambtenaren die het houden van toezicht als dagelijkse taak hebben (de 2019-groep). De zorg is dat, zodra meer ambtenaren kunnen melden, er een groter risico is op zowel een toename van meldingen van slechte kwaliteit als vals positieve meldingen. Het belang van expertise over het fenomeen ondermijning en dagelijks zicht op het veld werd aangemerkt als niet te onderschatten. Bovendien zijn er zorgen over de rol van de ambtenaar in de rol van 'opsporing' (of dat zo gaan ervaren), dat voor velen niet tot hun primaire taak hoort. Dit heeft mogelijk effect op de verhouding tussen gemeente en inwoners. Men zou kunnen zeggen dat dit voor het melden in het algemeen geldt, echter zou de MeV-app mogelijk drempelverlagend kunnen werken onder de brede groep ambtenaren.

Daarnaast zijn er zorgen over privacy en veiligheid; tijdens de sessie werd bijvoorbeeld onduidelijk via welk device ambtenaren gebruik kunnen maken van de app en hoe lang gegevens bewaard kunnen worden en wat de risico's zijn als gegevens toch niet helemaal verwijderd blijken. Er werd tot slot een belangrijke vraag gesteld over de effectiviteit van de app; het is momenteel niet duidelijk of gebruik van de app **meer** meldingen oplevert dan melden via e-mail of telefoon, en ook is niet duidelijk of de **kwaliteit** van meldingen beter is via de app dan via andere kanalen.

7. Aanbevelingen vanuit de sessie

Tijdens de sessie zijn een aantal aandachtspunten geformuleerd door de aanwezigen:

- 1) Verstrek duidelijkheid over de bewaartermijn van gegevens, en daarbij hoelang het duurt voor de ingevoerde gegevens uit de app verwijderd worden alvorens deze op de servers worden opgeslagen – dit aandachtspunt is in lijn met punt 3.4 uit de DPIA, waarin wordt aangegeven dat de gemeente nog een verantwoordelijke dient aan te wijzen voor het handhaven van de bewaartermijnen zoals in de archiefwet gespecificeerd. De vraag die tijdens de sessie nog onbeantwoord is, is of er reeds navolging gegeven is aan dit punt uit de DPIA.
- 2) Verstrek duidelijkheid over de manieren waarop (de data in) de MeV-app beveiligd is – dit is in lijn met punt 3.5 uit de DPIA, waarin wordt aangegeven dat de gemeente nog een aantal extra zaken moet opnemen in hun beveiligingsbeleid. Het gaat dan om: *een datalekkenprotocol, het opnemen van een verwerkingsregister, veiligstellen van back-ups, controle op de juistheid van ingevoerde gegevens en informeren van betrokkenen over gegevensverwerking*. De vraag die tijdens de sessie nog onbeantwoord is, is in hoeverre er reeds navolging gegeven is aan dit punt uit de DPIA.
- 3) Controleer de effectiviteit van de app en toets periodiek of de app van meerwaarde is of wordt bevonden voor het effectief registreren van zinvolle meldingen.
- 4) Creëer helder beleid en technische ingrepen om de MeV-app op de privételefoon niet mogelijk te maken.
- 5) Zorg blijvend voor de toegankelijkheid van het melden via andere kanalen.

8. Aanbevelingen Filosofie in actie

Vanuit de ervaring en expertise van het team van Filosofie in actie komen de volgende aandachtspunten:

- a) Veiligheid van gegevens en kwaliteit bleken een belangrijke aanleiding om deze app als middel te verkennen. Vergelijk de veiligheid en kwaliteit met de mogelijkheid om het melden bij voorkeur **telefonisch** te laten gebeuren via een speciaal intern meldnummer, en alleen via de werktelefoon. Digitale middelen zijn nooit 100% gevrijwaard van een hack of datalek. Bij telefonisch melden via een vaste lijn met beveiligde werktelefoons is de kans op onderscheppen of lekken van informatie kleiner.
- b) De **effectiviteit** van het middel staat ter discussie; reflecteer op de noodzaak van het gebruik van de MeV-app voor het doorgeven van meldingen en op de gevolgen voor het melden als het gebruik van de app helemaal zou worden stopgezet. In het kader hiervan is het een overweging om een pilot te starten waarin melden de app vergeleken wordt met andere vormen van melden (bijv. telefonisch) en een analyse te maken van de resultaten.
- c) Maak heel helder wat de mogelijke **risico's** zijn van het uitbreiden van de app naar alle ambtenaren – het is op dit moment niet helder hoe uitbreiding zowel de **kwaliteit** als de **kwantiteit** van meldingen zal beïnvloeden.
- d) Afhankelijkheid van een app maakt het meldsysteem mogelijk kwetsbaar; behalve veiligheids- en privacyrisico's die iedere digitale techniek met zich meebrengt, is de gemeente afhankelijk van de leverancier voor de technische ondersteuning van de app.
- e) Tot slot loopt de gemeente bij vergaande inzet van de app en als die als duidelijk voorkeurskanaal tot melden wordt ingezet mogelijk meldingen mis van medewerkers die niet voldoende digitale vaardigheden bezitten of liever via niet digitale wegen willen melden.

ⁱ <https://zoek.officielebekendmakingen.nl/stb-2019-346.html#d17e13234>