Haalbaarheid van een anoniem misdaadmeldpunt via het Internet

Een quickscan

Auteurs:

Jaap-Henk Hoepman
Bert-Jaap Koops
Wouter Lueks

Dit onderzoek is uitgevoerd door het Privacy & Identity Lab (http://www.pilab.nl/), hierbij juridisch vertegenwoordigd door de Radboud Universiteit Nijmegen.

Management Samenvatting

De onafhankelijke Stichting M. exploiteert sinds 2002 de meldlijn 'Meld Misdaad Anoniem', waar mensen per telefoon anoniem informatie kunnen geven over misdrijven.

Dit onderzoeksrapport geeft antwoord op de vraag of het technisch, juridisch en organisatorisch ook mogelijk is om de anonimiteit van melders te garanderen bij meldingen via Internet. Daarnaast is onderzocht wat de mogelijke voor- en nadelen van melden via Internet zijn voor de hoeveelheid en kwaliteit van de meldingen. Ook is in normatieve zin gekeken naar de rol die deze meldingen spelen in de strafvordering en in het maatschappelijk verkeer.

De resultaten van dit onderzoek zijn gebaseerd op een literatuurstudie, een interview met Stichting M. en een expert workshop.

Bij het verkennen van de normatieve aspecten van een anoniem Internetmeldpunt is de vraag gesteld of de inrichting van een anoniem meldpunt proportioneel is, is gekeken naar het risico van function creep, en is het effect van een publiek-private samenwerking bij zo'n meldpunt geanalyseerd.

Voor het bepalen van de technische haalbaarheid zijn de algemene risico's die kleven aan een Internetmeldpunt geanalyseerd. Vervolgens is een zestal mogelijke technische inrichtingen van een Internetmeldpunt getoetst tegen een aantal criteria die betrekking hebben op de anonimiteit, kwaliteit en gebruikersvriendelijkheid.

De juridische analyse heeft zich gericht op de verwerking van persoonsgegevens door het meldpunt, de positie van anonieme meldingen in het strafrecht, en de juridische mogelijkheden voor opsporingsdiensten om de identiteit van melders te achterhalen. Ook is gekeken naar aansprakelijkheidsrisico's voor het meldpunt, en de hoeveelheid en kwaliteit van meldingen vanuit juridisch perspectief.

Tenslotte is gekeken naar de organisatorische aspecten die van invloed zijn op de anonimiteit en kwaliteit van een Internetmeldpunt. Aandachtspunten waren het (technisch) beheer, de noodzaak van regelmatige audits, aandacht voor de integriteit van het personeel en de werkomgeving, en de invoeringsstrategie.

Onze belangrijkste conclusies wat betreft de haalbaarheid van een anoniem Internetmeldpunt, en de te verwachten voor- en nadelen daarvan, worden hieronder kort samengevat.

Wij concluderen dat een technisch voldoende veilige inrichting van een anoniem Internetmeldpunt geen sinecure is. Anonimiteit van een melder is lastiger te garanderen dan voor een telefonisch meldpunt. Interactiviteit van het meldpunt (d.w.z. de mogelijkheid om direct een dialoog met de melder aan te gaan) is essentieel om de kwaliteit (en anonimiteit) van de melding te garanderen. Een smartphone app of een web-gebaseerde chat toepassing voldoen om die reden het beste aan de criteria, maar kennen nog wel technische beperkingen. Vanwege de hoge complexiteit verwachten wij dat de kosten voor het inrichten van zo'n Internetmeldpunt hoog zullen zijn. Nader onderzoek naar een specifieke inrichting van een dergelijke smartphone app of zo'n web-gebaseerde chat toepassing, en daaraan verbonden risico's, is gewenst.

Vanuit juridisch perspectief is het verschil tussen een Internetmeldpunt en een telefonisch meldpunt minder groot. Zolang de Instructie Meld Misdaad Anoniem van het College van Procureurs-Generaal ook van toepassing wordt verklaard op een Internetmeldpunt, vormen de Wet bewaarplicht telecommunicatiegegevens en het zetten van Internettaps slechts een beperkt risico. Wel kan een laagdrempelig Internetmeldpunt tot ongewenste neveneffecten leiden, zoals schadeclaims en onrechtmatigedaadsacties. Ook de waarde van anonieme meldingen in het strafproces kan daardoor verminderen.

In organisatorische zin is de grotere technische complexiteit van een Internetmeldpunt ook een uitdaging. Het kennisniveau van de medewerkers zal hoger moeten liggen, en aan het beheer worden hogere eisen gesteld. Regelmatige audits zijn essentieel om de anonimiteit te blijven garanderen. Zoals gezegd verwachten wij geen daling van de kwaliteit van de meldingen bij een Internetmeldpunt. Over de te verwachten hoeveelheid meldingen die via een Internetmeldpunt binnen kunnen komen is echter weinig te zeggen. Eventuele invoering van een Internetmeldpunt zou daarom gefaseerd plaats moeten vinden, te beginnen met een pilot. Om de meerwaarde van een Internetmeldpunt ten opzichte van het reeds bestaand telefonisch meldpunt te

kunnen bepalen, lijkt het verstandig eerst een breed gedragen nulmeting naar de kwaliteit van het telefonisch meldpunt op te maken.

Wat betreft het anoniem melden van misdrijven blijkt dat er een reëel risico bestaat op function creep bij een meldpunt, zowel voor wat betreft het type misstanden dat wordt gemeld als voor het gebruik buiten de opsporing van anonieme meldingen die in politiebestanden terechtkomen. Een brede reflectie op deze ontwikkeling is gewenst, die zou moeten leiden tot het opstellen van een proportionaliteitstoets voor anonieme meldpunten. In een klimaat waarin politiële databanken op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet, is het belangrijk om terughoudend te zijn met het voeden van politiële databanken met ongecontroleerde informatie. Dit pleit voor terughoudendheid bij het faciliteren van anonieme meldingen.

Management Summary

Since 2002 the independent foundation Stichting M. operates the hotline "Meld Misdaad Anoniem ' (Report Crime Anonymously), where people can report criminal offences anonymously by phone.

This report answers the question whether it is technically, legally and organisationally possible to guarantee the anonymity of informants when the Internet is used to file reports instead. In addition, we investigated the possible advantages and disadvantages of reporting via the Internet for the quantity and quality of the reports. Also, we have looked at the role such reporting plays in criminal proceedings, and in society at large, from a normative perspective.

The results of this study are based on a literature review, an interview with Stichting M. and an expert workshop.

When exploring the normative aspects of an anonymous Internet hotline we studied whether the establishment of an anonymous hotline is proportional, we looked at the risk of function creep, and analysed the effect of a public private partnership in such a hotline.

To determine the technical feasibility , we analysed the general risks associated with an Internet hotline. Subsequently, six possible technical designs of an Internet hotline were tested against a number of criteria relating to anonymity, quality and user-friendliness.

The legal analysis focused on the processing of personal data by the hotline, the role of anonymous reports in criminal law, and the legal possibilities for investigators to retrieve the identity of the anonymous informants. We also looked at liability issues for the hotline, and the quantity and quality of anonymous reports from a legal perspective.

Finally, we looked at the organizational aspects that affect the anonymity and quality of an Internet hotline. Attention was paid to (technical) management, the need for regular audits, the integrity of personnel, the work environment, and the implementation strategy.

Our main conclusions regarding the feasibility of an anonymous Internet hotline and the expected advantages and disadvantages are summarized briefly below.

We conclude that technically speaking a sufficiently secure design of an anonymous Internet hotline is not easy. Anonymity of an informant is harder to ensure compared to a telephone hotline. Interactivity of the hotline (i.e. the opportunity to directly engage in dialogue with the informant) is essential to ensure quality (and anonymity) of the report. For that reason, a smartphone app or a web-based chat application meet the requirements best, although these do still have technical limitations. Due to the high complexity we expect that the cost of setting up such an Internet hotline will be high. Further study of a more detailed design of such smartphone app or web-based chat application, and the associated risks, is necessary.

From a legal perspective the difference between an Internet and a telephone hotline is less significant. As long as the instruction "Meld Misdaad Anoniem" of the Board of Attorneys-General is also made applicable to an Internet hotline, data retention regulation and Internet taps pose a limited risk. An easily accessible Internet hotline can lead to undesirable side effects however, such as claims for incurred damages and tort actions. The value of anonymous reports in criminal cases may decrease as a result.

In organizational terms, the increased technical complexity of an Internet hotline also poses a challenge. Staff must be properly trained, and more stringent demands will be imposed on technical support. Regular audits are essential for a continuous protection of anonymity. As said before we do not expect any decline in the quality of the reports when using an Internet hotline. However, it is hard to estimate the expected number of reports that will be received through an Internet hotline. The introduction of an Internet hotline would therefore have to proceed in stages, starting with a pilot. To determine the value of an Internet hotline compared to the existing telephone hotline, it appears to be wise to perform a well founded baseline study on the quality of the telephone hotline first.

As for the reporting of crime using anonymous hotlines, there appears to be a real risk of function creep, both with regard to the type of criminal activity that is reported as for the storage of information from anonymous reports beyond criminal investigations in police files. A broad reflection on this development is desired, which should lead to the establishment of a proportionality test for anonymous hotlines. In a climate where police databases are used in a rather non-transparent man-

ner for purposes other than criminal investigations, it is important to show restraint when feeding police databases with uncontrolled information. This calls for restraint in facilitating anonymous reporting.

Inhoudsopgave

Hoofdstuk 1

Inleiding

De onafhankelijke Stichting[1] M. exploiteert (onder meer) de meldlijn 'Meld Misdaad Anoniem', waar mensen anoniem informatie kunnen geven over misdrijven. Hierbij is de anonimiteit van de melder bij Stichting M. van hoofdbelang. Naar aanleiding van een anonieme telefonische melding maakt de stichting een 'call' (schriftelijke melding/verslag) aan en stuurt deze door naar publieke en private partners, zoals de politie en andere opsporingsdiensten. De partners zijn verantwoordelijk voor wat er met de melding gebeurt.

In september is stichting M. gestart met een pilot die het mogelijk maakt dat burgers, bij een telefonische melding, anoniem ook aanvullend beeldmateriaal kunnen sturen naar de stichting. Meer in het algemeen wordt verondersteld dat, indien de anonimiteit kan worden gegarandeerd, meldingen via Internet een goede aanvulling kunnen zijn op de mogelijkheid tot telefonisch melden. Vooral omdat de verwachting is dat de drempel voor melden lager ligt dan die voor telefonisch melden.

De minister heeft aan de Tweede Kamer[2] een onderzoek toegezegd naar de mogelijkheid van melden via Internet, waarbij de kwaliteit van de meldingen zo goed mogelijk geborgd is en de anonimiteit van de melder gegarandeerd blijft. Hierbij moet beoordeeld worden of (ook) bij meldingen via Internet de anonimiteit van de melder vanuit technisch, juridisch en organisatorisch perspectief gegarandeerd kan blijven. Ook moet het onderzoek een overzicht geven van mogelijke of verwachte voor- en nadelen van melden via Internet voor de hoeveelheid en de kwaliteit van de meldingen.

1.1 Onderzoeksopzet

Het voorliggende rapport vult deze toezegging van de minister in.

[1] Stichting M. heet sinds 1 januari 2014 NL Confidential. Omdat in een groot aantal stukken waar dit rapport naar refereert nog gesproken wordt over stichting M., en het verwarrend is om met twee verschillende namen naar dezelfde entiteit te verwijzen, kiezen wij ervoor om ook in dit rapport de oude naam te gebruiken.

[2] Kamerstukken II, 29 628, nr. 400, p. 2.

Dit leidt tot de volgende doelstelling van het voorgestelde onderzoek: het in kaart brengen van argumenten die relevant zijn voor de beoordeling of het wenselijk en haalbaar is om anonieme meldingen via Internet te doen plaatsvinden.

De vraagstelling die centraal staat is: In hoeverre is het technisch, juridisch en organisatorisch mogelijk om de anonimiteit van melders te garanderen bij meldingen via Internet? Wat zijn, op technisch, juridisch en organisatorisch vlak, de mogelijke voor- en nadelen van melden via Internet voor de hoeveelheid en kwaliteit van de meldingen en voor de rol die deze meldingen spelen in de strafvordering en in het maatschappelijk verkeer?

1.1.1 Onderzoeksvragen

Het onderzoek is geordend aan de hand van de volgende deelvragen die tezamen een antwoord geven op de algemene vraagstelling.

1. In hoeverre is het haalbaar om de anonimiteit van melders te garanderen bij meldingen via Internet?
    - In hoeverre is dit technisch mogelijk?
        - Welke partijen zijn in staat (en hebben de motieven) om de anonimiteit van een melding te doorbreken?
        - Welke mogelijke technische inrichtingen zijn er voor een anoniem meldpunt?
        - In welke mate beschermen deze de anonimiteit tegen de hierboven genoemde partijen? Wat zijn de eventuele nadelen (qua kosten of functionaliteit)?
    - In hoeverre is dit juridisch mogelijk?
        - Hoe verhoudt een anoniem meldpunt zich tot dataretentiewetgeving en tot bevoegdheden van opsporingsdiensten en inlichtingen- en veiligheidsdiensten om (verkeers)gegevens te vorderen?
        - Zijn er aansprakelijkheidsrisico's voor het meldpunt in gevallen waarin anonimiteit van melders wordt doorbroken?

    - Welke juridische maatregelen kunnen helpen om de anonimiteit van melders te garanderen?
  - In hoeverre is dit organisatorisch mogelijk?
    - Welke organisatorische maatregelen kunnen helpen de anonimiteit van melders te garanderen?
  - Wat betekent de combinatie van technische, juridische en organisatorische mogelijkheden en obstakels voor de anonimiteit van meldingen via Internet?
2. Welke zijn, op technisch, juridisch en organisatorisch vlak, de mogelijke of verwachte voor- en nadelen van anoniem melden via Internet:
  - voor de hoeveelheid van de meldingen?
  - voor de kwaliteit van de meldingen?
  - voor de rol van anonieme meldingen in de opsporing?
  - voor de rol van anonieme meldingen in het maatschappelijk verkeer?

Merk op dat anonimiteit geen zwart/wit-begrip is en het niet zinvol is om te kijken naar het "garanderen" van anonimiteit. Absolute anonimiteit zal (vrijwel) onmogelijk zijn, en is als zodanig ook niet nodig voor een werkbaar systeem van anoniem melden. Relevanter is het te kijken naar de mate waarin anonimiteit bewerkstelligd zou kunnen worden.

Het Internet kent een eigen dynamiek in het maatschappelijk verkeer ten opzichte van de traditionele telefonie, die verder gaat dan een invloed op kwantiteit en kwaliteit van het communicatieverkeer. Het Internet faciliteert, en beïnvloedt daarmee, de manier waarop communicatie en sociale contacten plaatsvinden. Het is daarom van wezenlijk belang voor een onderzoek naar de mogelijkheden van anoniem melden via Internet om ook de mogelijke gevolgen in kaart te brengen voor de rol van anoniem melden in het strafrecht en de maatschappij in bredere zin. In een apart hoofdstuk wordt in dit rapport op dit normatieve aspect ingegaan.

1.1.2 Aanpak

Vanwege de beperkte beschikbare doorlooptijd heeft het onderzoek zich beperkt tot een 'quick scan', waarbij de ervaring van stichting M. betrokken is middels een interview (dat plaatsvond op dinsdag 7 Januari 2014) en de expertise van andere organisaties die ervaring hebben met (anonieme) publieke meldingen betrokken is middels een expert meeting die op vrijdag 31 januari 2014 heeft plaatsgevonden (zie bijlage C). Daarnaast heeft een literatuurstudie plaatsgevonden en zijn verschillende bestaande systemen met vergelijkbare functionaliteit (met name voor klokkenluiders) onderzocht.

Het concept rapport is aan stichting M. ter controle op feitelijke onjuistheden voorgelegd.

1.2 Leeswijzer

We beginnen het rapport met een beschrijving van de belangrijkste uitgangspunten van ons onderzoek. De normatieve aspecten van de wenselijkheid van een anoniem Internetmisdaadmeldpunt worden onderzocht in hoofdstuk 3. In hoofdstuk 4 beschrijven we de mogelijke technische inrichtingen van een anoniem Internetmeldpunt, en gaan we in op de risico's daarvan. Hoofdstuk 5 belicht de voor- en nadelen van anoniem melden via het Internet vanuit het juridisch perspectief. Tenslotte behandeld hoofdstuk 6 de organisatorische aspecten die relevant zijn voor het beantwoorden van de onderzoeksvraag. We eindigen dit rapport met een aantal conclusies en aanbevelingen waarin de onderzoeksvragen beantwoord worden.

Hoofdstuk 2

Uitgangspunten

Zoals in de inleiding reeds beschreven, bestaat er al een meldpunt waar burgers telefonisch melding kunnen doen van een misdrijf. In dit hoofdstuk zal kort de werking van en ervaringen met dit telefonisch meldpunt beschreven worden, en iets verder ingegaan worden op de aanleiding om over een Internetmeldpunt na te denken. Dit om ons onderzoek naar de mogelijkheid en wenselijkheid van een vergelijkbaar meldpunt via Internet in het juiste perspectief te plaatsen.

2.1 Huidige situatie

Sinds december 2003 exploiteert Stuichting M. het meldpunt "Meld Misdaad Anoniem" [3]. Via het meldpunt kunnen burgers telefonisch, via een 0800 nummer, anoniem informatie doorgeven over ernstige strafbare feiten. Getrainde telefonisten, in dienst van de stichting, beantwoorden binnenkomende gesprekken en maken een verslag van iedere bruikbare melding.

Stichting M. is een private partij, die naast publieke partijen (zoals de KLPD, de FIOD, de AIVD) ook private partijen (zoals het Verbond van Verzekeraars en de energienetbeheerders) als afnemers[1] kent. De stichting zet een verslag van binnenkomende meldingen door aan deze afnemers. Welke meldingen doorgegeven worden aan welke afnemers hangt af van de aard van de melding en de afspraken die met de individuele afnemers daarover zijn gemaakt. Zo worden bijvoorbeeld meldingen over illegale hennepkwekerijen ook doorgegeven aan de energienetbeheerders. Of een melding ernstig genoeg is om anoniem te doen dan wel af te handelen wordt dus bepaald door Stichting M., haar afnemers en natuurlijk de beller zelf (door te beslissen om contact op te nemen met het meldpunt).

Meldingen worden via 'Meldnet' verstrekt aan die afnemers waarvoor de informatie is bestemd. Meldnet is een speciaal voor Stichting M. voor dit doel ontworpen systeem. In de rest van dit onderzoek gaan we er van uit dat ook voor melden via Internet de uiteindelijke meldingen via Meldnet aan de afnemers worden doorgegeven. In die zin verandert melden via Internet dus niets aan de 'backoffice' van Stichting M., en dus ook niets aan het koppelvlak waarmee de afnemers de meldingen ontvangen.

Stichting M. heeft zowel de computersystemen als de telefonie geoutsourced aan Pink Elephant [25]. Beide worden door Stichting M. van Pink Elephant afgenomen als een clouddienst. Hierbij is ook de mogelijkheid ingebouwd voor medewerkers om vanuit huis te werken.

De unique selling point van het meldpunt is haar garantie van anonimiteit. Daar wordt dus zwaar door Stichting M. op ingezet. Bij telefonisch binnenkomende meldingen wordt de anonimiteit van zowel de melder als de melding als volgt gewaarborgd.

- Meldingen worden aangenomen door getrainde telefonisten, die er voor zorgen dat het verslag van de melding anoniem is, en daarnaast concreet genoeg voor de afnemers om actie op te ondernemen.
- Een tweede lezer (ook in dienst van Stichting M.) controleert of het verslag voldoende anoniem is.
- Verslagen worden niet bewaard. Na goedkeuring van de tweede lezer wordt de melding via Meldnet (zie boven) doorgegeven aan de relevante afnemers. Er wordt geen registratie bijgehouden waaruit af te leiden is welke telefonist welke melding heeft aangenomen.
- Er is een Instructie Meld Misdaad Anoniem van het College van Procureurs-Generaal (CPG) waarin is vastgelegd dat verkeersgegevens (zoals de worden verzameld in het kader van de wet op de bewaarplicht) betreffende het meldpunt alleen worden opgevraagd in situaties van onmiddellijk dreigend levensgevaar, waarbij de gegevens alleen mogen worden gevorderd als de inlichtingen nodig zijn om het desbetreffende leven te redden [9].
- Het 0800 nummer van de dienst "Meld Misdaad Anoniem" wordt niet vermeld op de specificatie van de telefoonrekening van de melder.

[1] Door stichting M. partners genoemd.

Uit het interview met stichting M. komen ook de volgende significante punten naar voren.

- Ondanks de specifieke Instructie van het CPG ten aanzien van het meldpunt, probeert de politie incidenteel om via de stichting alsnog de identiteit van de melder te achterhalen.
- De indruk van Stichting M. is dat het telefonische kanaal door een diverse groep mensen wordt gebruikt, met als kanttekening dat jongeren duidelijk ondervertegenwoordigd zijn.
- De kwaliteit van de melding staat of valt met de mogelijkheid een dialoog te voeren met de melder. In één enkel telefoongesprek zijn de telefonisten in staat om een vertrouwensband met de melder op te bouwen, die hen in staat stelt de serieusheid van de melding in te schatten, en er voor te zorgen dat de melding voldoende aanknopingspunten voor vervolgstappen bevat. Subtiele signalen tijdens het gesprek zelf, zoals omgevingsgeluiden, of hoe de melder overkomt tijdens het gesprek, kunnen hierbij ook behulpzaam zijn.
- Naast de kwaliteit is ook de anonimiteit van de melding gebaat bij een dialoog met de melder. Zo kan bijvoorbeeld bepaald worden of de melder wellicht de enige is die van het gemelde feit op de hoogte kan zijn. In dat geval is de melder in feite niet anoniem.
- Documenten als ondersteuning van een melding zijn zelden gewenst, omdat deze vaak identificerende kenmerken en/of niet de juiste informatie bevatten. Soms ontvangt de stichting meldingen per post. Deze worden direct vernietigd.

Niet onbelangrijk, ook in de context van het voorliggende onderzoek, is de bruikbaarheid van de meldingen zoals die op dit moment via het telefonisch meldpunt binnenkomen. Hierover verschillen de meningen. De Stichting M. schat de bruikbaarheid van de door haar doorgegeven meldingen aanzienlijk hoger in dan hierover door onderzoek binnen de politiekorpsen [19] wordt gerapporteerd. Volgens Stichting M. gaf zij in 2012 13.660 meldingen door aan de politie, waarvan 92% bruikbaar was. 68% van deze bruikbare meldingen werden in onderzoek genomen, waarvan 32% resultaat opleverde. Van Kuik e.a. [19] geven echter de volgende cijfers. Op de bij de politie binnengekomen meldingen is in 35% van de gevallen actieve actie ondernomen. Hiervan heeft 32% (dus 11% van alle aan de politie doorgegeven meldingen) in meer of mindere mate bijgedragen aan de opsporing in de zaak.

Bovenstaande is slechts een zeer korte samenvatting van de meest relevante gegevens over de opzet en werkwijze van Stichting M., zoals zij het meldpunt "Meld Misdaad Anoniem" exploiteert. Voor verdere informatie verwijzen we graag naar het onderzoek van Boes [3] uit 2010, en van Kuik e.a. [19] uit 2012.

2.2 Internet als nieuw kanaal

Het denken over Internet als een nieuw kanaal voor het anoniem melden van misdrijven is voornamelijk ingegeven door een zekere mate van opportunisme. Het inzetten van Internet als nieuw kanaal biedt kansen op twee vlakken. Ten eerste verwacht Stichting M. dat Internet een lagere drempel biedt om een melding te doen (een telefoongesprek is intiemer dan een afstandelijker contact via Internet). Ook de politiek lijkt die gedachte toegedaan.[2] Ten tweede constateert de stichting dat jongeren duidelijk minder melding maken van misdrijven via het op dit moment telefonisch aangeboden meldpunt. De verwachting is dat via Internet een ander publiek (en dan met name jongeren) aangeboord kan worden. Wel dient opgemerkt te worden dat ons geen onderzoeken bekend zijn die deze verwachte voordelen van een Internetmeldpunt met concrete cijfers onderbouwen.

Daarnaast is stichting M. zich er van bewust dat het gebruik van Internet als nieuw kanaal ook tot nieuwe risico's of een andere inschatting van dergelijke risico's leidt. Dit is niet beperkt tot de technische risico's die het gebruik van Internet kan hebben ten aanzien van de anonimiteit van de melder.

Zo kan een lagere drempel (één van de doelstellingen van een eventueel in te richten Internet-gebaseerd meldpunt) leiden tot een grote toestroom van meldingen. Deze stroom moet niet alleen door het meldpunt zelf maar ook door de afnemers verwerkt kunnen worden. Als bij de afnemers een bottleneck ontstaat, rijst de vraag waar de beslissing wordt genomen om een melding op te nemen, door te zetten of op te pakken. Moet de inrichter van het meldpunt, op dit moment een private partij, een keuze maken over de ernst van een binnenkomende melding om zo de afnemers te ontlasten. Of is dit een verantwoordelijkheid van de afnemers zelf?

Daarnaast kan een lagere drempel leiden tot een lagere kwaliteit van de meldingen. Afhankelijk van de inrichting van het meldpunt via Internet kan dit opgevangen worden door het meldpunt zelf. In andere gevallen zal dit leiden tot lagere kwaliteit van de meldingen zoals die uiteindelijk bij de afnemers terecht komen

Juist ook deze vragen en afwegingen worden in dit voorliggende onderzoek nader geanalyseerd.

[2] Kamerstukken II, 29 628, nr. 368, p. 6.

Hoofdstuk 3

Normatieve aspecten: een reflectie op anoniem Internetmelden

Zoals in het vorige hoofdstuk al is aangegeven, is het denken over het Internet als nieuw kanaal voor anonieme misdaad meldingen vooral ontstaan uit de verwachting dat een Internetmeldpunt mogelijk een lagere drempel opwerpt voor anonieme meldingen, en dat daarmee ook een andere, vooral jongere, doelgroep anonieme meldingen zal gaan doen. Bij de beoordeling van de wenselijkheid en de verschillende mogelijkheden om een anoniem Internetmisdaadmeldpunt op te richten moeten naast technische, juridische en organisatorische factoren ook normatieve aspecten in bredere zin worden onderzocht. Een normatieve reflectie was niet in de oorspronkelijke vraagstelling van de onderzoeksaanvraag besloten; de Minister heeft de Kamer een onderzoek toegezegd 'naar hoe [anoniem melden via internet] kan worden geregeld waarbij de kwaliteit van de meldingen zo goed mogelijk geborgd is en de anonimiteit van de melder gegarandeerd blijft'[1], zonder de vraag of dit in algemene zin wenselijk zou zijn. Hoewel de Kamer beseft dat een Internetmeldpunt 'meer inhoudt dan even een websiteje bouwen'[2], lijkt men vooral te denken aan de technisch-organisatorische borging van anonimiteit en niet aan de normatieve kant van een anoniem Internetmeldpunt. Daarmee wordt volgens ons miskend dat het Internet een eigen dynamiek kent in het maatschappelijk verkeer ten opzichte van de traditionele telefonie, die verder gaat dan een invloed op kwantiteit, kwaliteit en identificeerbaarheid van het communicatieverkeer. Het Internet faciliteert, en beïnvloedt daarmee, de manier waarop communicatie en sociale contacten plaatsvinden. Het is in dat licht van wezenlijk belang voor een onderzoek naar de mogelijkheden van anoniem melden via Internet om te wijzen op de mogelijke gevolgen van de rol van anoniem melden voor maatschappelijke processen in bredere zin.

De onderzoekers hebben er daarom voor gekozen, naast een overzicht van technische, juridische en organisatorische aspecten, eerst te wijzen op enkele normatieve aspecten die in elk geval om nadere reflectie vragen, alvorens tot de oprichting van een anoniem Internetmisdaadmeldpunt zou kunnen worden overgegaan. In dit hoofdstuk bespreken wij vier normatieve aspecten: de rechtsstatelijke eis van proportionaliteit, het bestaan van een 'klikcultuur', het reële risico van function creep en de rol van private partijen in de strafrechtspleging. Deze aandachtspunten zouden een startpunt moeten zijn van een bredere reflectie op de effectiviteit, rechtvaardiging en proportionaliteit van anonieme misdaadmeldpunten. Daarnaast bevelen wij aan dat in het kader van de rechtvaardiging van mogelijke inbreuken op de grondrechten van degenen over wie wordt gemeld, naast de technische bescherming van de melder ook effectief aandacht wordt besteed aan technische en organisatorische bescherming van degenen die daarmee verdacht worden gemaakt.

3.1 Proportionaliteit

Vanuit rechtsstatelijk perspectief is het wezenlijk dat een adequate proportionaliteitstoets wordt uitgevoerd, die aan de orde is wanneer de overheid maatregelen neemt die een inbreuk vormen op grondrechten. In dit geval gaat het om de grondrechten op privacy, op gegevensbescherming, non-discriminatie en de onschuldpresumptie in brede zin. Terwijl degene die gebruik maakt van een anoniem meldpunt daarmee bijzondere bescherming verkrijgt, zijn de rechten van degene over wie verdenkingen of andere negatieve informatie wordt gemeld in het geding. Voor zover het gaat om een natuurlijk persoon worden persoonsgegevens verwerkt en afhankelijk van de inhoud van de melding is een inmenging van de privacy aan de orde (er wordt bijvoorbeeld informatie gegeven over het privéleven, de thuissituatie, levenswandel die langs vertrouwelijke weg is verkregen), negatieve beeldvorming over personen met een andere etnische achtergrond of seksuele voorkeur kan leiden tot het zwartmaken van bepaalde

[1] Kamerstukken II 2012/13, 29 628, nr. 400, p. 2, cursivering toegevoegd.

[2] Kamerstukken II 2012/13, 29 628, nr. 368, p. 6.

categorieën individuen die daardoor een grotere kans lopen aan nader onderzoek te worden onderworpen, en de desbetreffende persoon kan zich niet verweren tegen de aantijgingen totdat het de politie behaagt om hem daarvan op de hoogte te brengen. Hoewel de onschuldpresumptie juridisch-technisch gezien pas ingaat op het moment dat sprake is van strafrechtelijke vervolging in enge zin, moeten erkend worden dat anonieme verdachtmakingen ook kunnen leiden tot de inzet van strafvorderlijke maatregelen in de vroegsporing, die op gespannen voet staan met de rechtsstatelijke achtergrond van de onschuldpresumptie. In samenhang met het feit dat mensen zich niet kunnen verdedigen totdat zij formeel als verdachte worden aangemerkt, moet worden vastgesteld dat hier sprake is van mogelijke inbreuken op grondrechten die rechtvaardiging behoeven. Die rechtvaardiging zal allereerst moeten bestaan uit de proportionaliteitstoets: weegt het voordeel dat wordt behaald met het legitieme doel van misdaadbestrijding op tegen de mogelijke inbreuken? (Zie hierover de recente opinie van de Artikel 29-Werkgroep over de toepassing van de noodzakelijkheids- en proportionaliteitstoets in de strafvordering [24].) Daarbij rijst de vraag naar de effectiviteit van anoniem melden. Is er empirisch onderzoek beschikbaar en wordt empirisch onderzoek voorzien, dat toestaat om uitspraken te doen over effectiviteit van het meldpunt, met inachtneming van bijvoorbeeld de volgende onderscheidingen: welk type klachten (burenruzies of bouwfraude), welk type klagers (allochtoon, autochtoon, achtergrond, opleiding, rancuneus, gefrustreerd), in wat voor domeinen (commune criminaliteit, belasting- of sociale-zekerheidsfraude, misbruik van voorkennis)? Daarbij gaat het dan ook steeds om de vraag in hoeverre de melding niet op andere wijze had kunnen plaatsvinden, waarbij geen of in mindere mate sprake is van de aantasting van grondrechten. Dit alles is niet alleen van belang bij de vraag naar de proportionaliteit maar ook—mocht duidelijk zijn dat in bepaalde gevallen wel degelijk sprake is van een gerechtvaardigde inbreuk—bij de vraag naar de waarborgen die worden getroffen om de inbreuken te beperken en in rechte aanvechtbaar te maken. Het is goed mogelijk dat in bepaalde gevallen anoniem melden heel zinvol is, vanwege de machtsverhoudingen die in het spel zijn, terwijl het in andere gevallen juist ongewenste machtsverhoudingen verder versterkt. Een gedetailleerde en onderbouwde beoordeling van de proportionaliteit is binnen het kader van deze quickscan niet mogelijk en zou daarom in nader onderzoek moeten worden uitgevoerd.

3.2 Een klikcultuur?

De oprichting en het functioneren van de Meld Misdaad Anoniem-telefoonlijn is door velen geplaatst in een breder kader van een mogelijke 'klikcultuur'. Vrij algemeen wordt onderkend dat de rol van anonieme meldingen in de maatschappij het afgelopen decennium of de afgelopen decennia is toegenomen. Zo begon NRC Handelsblad op 28 februari 2002 een stuk getiteld 'Nederland klikland' met de opmerking 'Nederland kent tientallen kliklijnen', en zo kopte cultuurfilosoof Hans Schnitzler in 2012: 'We leven in een "klikspaan boterspaan"-land' [26]. Buruma [7, p. 171] wijst op het kennelijk toenemende belang dat in het strafrecht wordt gehecht aan afgeschermde informanten, anonieme meldingen, anonieme aangifte en discrete meldingen van geheimhouders bij meldpunten.

Hoewel men het er wel over eens lijkt dat het anoniem melden van misdaad past in een bredere maatschappelijke tendens van anonieme meldingen, verschilt de waardering van deze tendens. Aan de ene kant zijn er mensen die de tendens als negatief ervaren en wijzen op de risico's voor de manier waarop we in de maatschappij met elkaar omgaan. Zo stelt criminologe Lissenberg in haar afscheidsrede dat anoniem informatie verstrekken het onderlinge wantrouwen bestendigt of vergroot. In die zin heeft volgens haar 'de introductie van meldlijn M. niet bijgedragen tot goed burgerschap' [21, p. 9].

Een vergelijkbaar geluid liet Kees Schuyt als voorzitter van het Landelijk Orgaan Wetenschappelijke Integriteit onlangs horen in een pleidooi tegen anoniem melden van wetenschapsfraude. 'Je geeft op die manier ruimte aan roddel en achterklap en creëert een sfeer van achterdocht en wantrouwen aan de universiteit. Integriteitsklachten kunnen op deze manier misbruikt worden om concurrenten uit te schakelen' [17]. Ook cultuurfilosoof Schnitzler plaatst anoniem melden van misstanden in het brede perspectief van het wantrouwen in een maatschappij die in tijden van identiteitscrisis 'de ander' zwart maakt [26].

Buruma wijst op de gevaren van deze tendens voor de strafrechtspleging. Reflecterend op de zaak Lucia de B. stelt hij dat de omgang met (valse of verkeerde) aangiften in de strafvordering aan verandering onderhevig is, mede vanwege het feit 'dat in de afgelopen 10 jaar een krachtige impuls is gegeven aan het belasteren van medeburgers. Ik denk in de eerste plaats aan het vergemakkelijken van anonieme tips en aangiften' [6, p. 694].

Naast de gevolgen van anoniem melden voor burgerschap, wijst Lissenberg ook op de mogelijke gevolgen voor de integriteit van bestuurlijk en bedrijfsmatig handelen. 'Geheime tips wakkeren het onderlinge wantrouwen aan, terwijl integriteit gebaat is bij vertrou-

wen. Een grotere openheid en ontvankelijkheid voor kritiek en een andere mentaliteit in de omgang met regeloverschrijdingen vergroten de integriteit van werkgevers en werknemers in een organisatie. ' [21, p. 17] Ook Buruma signaleert risico's voor de integriteit van de politie. Agenten kunnen een anonieme tip gebruiken om een 'bekende' na te trekken en zonder een juridisch adequate aanleiding over te gaan tot opsporingshandelingen in de hoop dat er iets boven water komt. Dit is 'problematisch omdat op deze manier vrij baan wordt gegeven aan agenten die met iemand een appeltje te schillen hebben.' [7, p. 207] In dat licht moet ook worden gewezen op het kleine maar niet verwaarloosbare risico dat de politie het meldpunt kan misbruiken om onrechtmatig verkregen informatie wit te wassen of om informanten af te schermen (zie verderop, par. 5.5).

Aan de andere kant zijn er mensen die de positieve kanten van de tendens van anoniem melden benadrukken. Zo bekritiseert Brinkhoff de uitspraken van Lissenberg omdat het niet duidelijk is waarop zij de verwachting baseert dat het onderling wantrouwen groeit: 'Even goed zou kunnen worden betoogd dat de invoering van de M-lijn het gevoel van veiligheid en vertrouwen van burgers (onder meer in politie en justitie) juist vergroot' [5]. Ook Boes [3, p. 25 e.v.] plaatst kanttekeningen bij de feitelijkheid van de door tegenstanders gehanteerde argumenten. Zij trekt een tegenovergestelde conclusie over de bredere effecten van de anonieme meldlijn op de maatschappij: ' Stichting M. bevordert de informele controle en versterkt daarmee de sociale structuren in de samenleving. Dit gebeurt niet alleen door de exploitatie van de anonieme meldlijn, ook de wijkgerichte acties van Stichting M. hebben daar een belangrijke rol in' [3, p. 4]. Zij concludeert dat M. juist een uiting is van goed burgerschap, omdat misdaadmelden niet klikken maar een burgerplicht betekent.

Ook de evaluatie van het proefproject Meld Misdaad Anoniem concludeerde op basis van een representatieve steekproef onder de bevolking dat de meldlijn in een behoefte voorziet en 'kan rekenen op een breed draagvlak onder de bevolking. (...) Opvallend is dat een zeer groot deel van de bevolking zich medeverantwoordelijk voelt voor de veiligheid in Nederland en het melden van misdaden als burgerplicht beschouwt' [2, p. 43]. Bij dat laatste is overigens niet duidelijk of dat ook het anoniem melden van misdaden betreft, en daar gaat het hier natuurlijk om. In een media-analyse van artikelen over meldlijn M. bleek dat weliswaar 'klikken' in de artikelen vaker werd genoemd dan 'melden' of 'tippen', maar, zo menen de onderzoekers desondanks, '[v]an een negatieve associatie lijkt in de berichtgeving echter geen sprake te zijn' [2, p. 30].

Hoewel sommigen zullen vinden dat de oprichting van een Internetmeldpunt meer een uitbreiding dan een substantiële verandering of versterking van het reeds bestaande telefonische meldpunt zou zijn, zal uit de volgende hoofdstukken blijken dat de verschillen tussen een telefonisch meldpunt en een Internetmeldpunt wellicht groter zijn dan gedacht. Daarom moet wel worden nagedacht wat de gevolgen zijn van een Internetmeldpunt voor de tendens van anoniem melden in het algemeen, in het licht van de lopende discussie tussen voor- en tegenstanders van de 'kliklijn'. Zoals in de workshop over een Internetmeldpunt werd opgemerkt: 'Je versterkt een klikcultuur, die we toch al een beetje hebben in Nederland.' Aangezien er verschillende perspectieven bestaan op de normatieve waardering van deze versterking van een 'klikcultuur', valt het aan te bevelen eerst een bredere maatschappelijke en politieke discussie te voeren over deze materie, alvorens men over zou gaan tot de oprichting van een Internetmeldpunt.

3.3 Function creep

Function creep is een term die in de sociale wetenschappen wordt gehanteerd voor het geleidelijk uitbreiden van de functionaliteit of toepassingen van systemen of gegevens. Een systeem dat voor een bepaald doel wordt ontwikkeld, wordt later vaak ook toegepast voor andere doelen; gegevens die voor het ene doel zijn verzameld, worden vervolgens ook gebruikt voor andere doelen. Hoewel er als zodanig niets mis lijkt met het uitbreiden van de toepassing van systemen of hergebruik van gegevens, gebeurt de uitbreiding vaak impliciet en zonder reflectie op de mogelijke neveneffecten en risico's van de nieuwe toepassingen—men denkt vaak dat de beheersmaatregelen die zijn getroffen voor het oorspronkelijke doel ook wel zullen werken voor het nieuwe doel. Wanneer het gaat om overheidshandelen is het uitbreiden van bevoegdheden of het nemen van maatregelen die inbreuken op grondrechten mogelijk maken wel degelijk een probleem, zoals in de inleiding reeds beschreven. Daarbij kan een legitimiteitstekort ontstaan (de oorspronkelijke juridische en democratisch gelegitimeerde basis dekt niet noodzakelijk ook de nieuwe toepassingen) en kunnen gaten in rechtsbescherming ontstaan omdat de nieuwe toepassing vaak in een andere context plaatsvindt, waarin andere regels en risico's spelen.

Function creep is een relevant aandachtspunt voor anonieme misdaadmeldingen. Het oorspronkelijke en hoofddoel van de anonieme meldlijn is om opsporing van misdrijven te faciliteren die anders onbekend zouden blijven, omdat mensen soms om uiteenlopende redenen geen aangifte of melding bij de politie willen doen. Waar het meldpunt primair een rol heeft om ernstiger vormen van criminaliteit in beeld te krijgen die anders onbekend zouden blijven, zou de norm in

de loop der tijd verlaagd kunnen raken wanneer ook minder ernstige strafbare feiten of een ruimer scala aan maatschappelijke misstanden wordt gemeld. Het is zaak dat gedegen empirisch onderzoek beschikbaar komt naar de vraag waarom en wat mensen anoniem melden: in hoeveel gevallen gaat het bijvoorbeeld om angst voor contact met de politie, angst voor represailles, om gemakzucht, of om frustratie of onvermogen die niets met te maken hebben met datgene of degene waarover wordt gemeld? Daar komt bij dat meldingen bij het telefonische meldpunt niet alleen worden gebruikt door de politie voor opsporingsdoelen, maar ook door andere overheidsdiensten en private partijen. Meldingen worden door het meldpunt doorgegeven aan onder andere sociale-zekerheidsdiensten, energienetbeheerders en het verbond van verzekeraars (Boes 2010, p. 48-53). De beslissingen die dergelijke afnemers nemen op basis van anonieme meldingen, vinden plaats in een andere context dan het strafproces. De bestaande jurisprudentie over de bruikbaarheid van meldingen, waarbij enige aanvullende informatie of verificatie wordt geëist alvorens de politie over mag gaan tot opsporingshandelingen, is hierop niet van toepassing. Dit roept vragen op over het beginsel van 'due process' in de andere contexten waarin beslissingen worden genomen over in anonieme meldingen genoemde individuen: vindt er hoor en wederhoor plaats? Is het voldoende transparant voor de betrokkene dat een beslissing mede is gebaseerd op een anonieme melding? Kan de betrokkene klagen over het gebruik van anonieme startinformatie? En voldoet het gebruik van anonieme misdaadmeldingen aan het subsidiariteitsbeginsel? Tegelijkertijd zijn hier verplichtingen uit het gegevensbeschermingsrecht aan de orde: op welke grondslag mag bijvoorbeeld de desbetreffende instantie de persoonsgegevens uit de melding verwerken en is hier nog sprake van een compatibel doel? Deze vragen verschillen overigens niet voor een eventueel op te richten Internetmeldpunt ten opzichte van het huidige telefonische meldpunt, en in deze quickscan kunnen wij ook niet ingaan op alle contexten waarin anonieme meldingen worden gebruikt. Het is wel van belang om deze vragen te beantwoorden bij de afweging om een Internetmeldpunt op te zetten, omdat daarbij zorgvuldig moet worden overwogen wie de mogelijke afnemers van meldingen zouden moeten zijn, en of de legitimiteit en rechtsbescherming van niet-opsporingsgerelateerd gebruik van anonieme meldingen wel voldoende gewaarborgd zijn.

Naast het gebruik voor andere doelen wanneer meldingen aan andere afnemers dan de politie worden gestuurd, is het vooral ook van belang om te bekijken welke rol anonieme meldingen spelen die aan de politie worden doorgegeven maar die buiten de opsporing in strikte zin worden gebruikt. Het strafrechtelijk systeem raakt meer en meer verweven met bestuursrechtelijke, en soms civielrechtelijke beslissingen, zoals gebiedsverboden en uithuisplaatsingen van kinderen. De opname van anonieme meldingen in politiesystemen kan allerlei consequenties hebben, ook zonder dat de melding leidt tot een opsporingshandeling. 'Politie- en justitiebestanden maken het mogelijk een klasse van permanent gestigmatiseerde personen te scheppen (...). Je hoeft echt niet veroordeeld te zijn om op grond van een analyse van bureau bibob geen vergunning te krijgen' [7, p. 209]. Het risico van stigmatisering door ongecontroleerde beschuldigingen in anonieme meldingen wordt aanzienlijke groter naarmate politiegegevens ook function creep ondergaan.

Tekenend voor function creep bij politiegegevens zijn twee politieke proefballonnen die recent werden opgelaten. De gemeenten Eindhoven en Tilburg willen zelf politiegegevens analyseren, omdat de politie daar niet altijd aan toekomt, zodat zij deze gegevens kunnen gebruiken bij onder andere het preventieve jeugdbeleid ('Steden runnen hun eigen "inlichtingendienst"', *Trouw*, 29 januari 2014). Staatssecretaris Teeven beoogt om de wet te veranderen zodat een verklaring omtrent het gedrag ook kan worden geweigerd louter op basis van politiegegevens en niet, zoals nu, op basis van justitiële gegevens omtrent een veroordeling of opgelegde OM-boete of -transactie[3]. Overigens kan naar huidig recht al een verklaring omtrent het gedrag worden geweigerd zonder dat een veroordeling of sanctie is opgelegd. Blijkens een uitspraak van de Raad van State[4] mag een verklaring omtrent het gedrag ook worden geweigerd op basis van justitiële gegevens over 'strafbare feiten ter zake waarvan een beslissing tot dagvaarding of seponering of een andere beslissing van het openbaar ministerie is genomen.' In dit geval had de weigering om een verklaring omtrent het gedrag af te geven tot gevolg dat de betrokkene geen baan kreeg. Politiegegevens gebaseerd op anonieme meldingen die via een opsporingsonderzoek leiden tot een dagvaarding of seponering van de zaak kunnen op deze manier ingrijpende gevolgen hebben. Dergelijke toepassingen van politiegegevens buiten de strafvordering raken burgers op een significante manier, door vergunningweigeringen, verzwaard toezicht door de jeugdzorg of het niet krijgen van een baan wegens het ontbreken van een verklaring omtrent het gedrag. Ook hier is het de vraag of er voldoende rechtsbeschermingsmaatregelen zijn die 'due process' waarborgen. Aangezien in deze situaties geen rechterlijk toezicht plaatsvindt, is het de vraag of getroffen burgers de betrouwbaarheid van politiegegevens die gebaseerd zijn op een anonieme melding wel kunnen aanvechten[5] en of er voldoende aan-

[3] Kamerstukken II 2013/14, 33 750 VI, nr. 99, p. 2

[4] ABRvS 29 januari 2014, ECLI:NL:RVS:2014:205.

[5] Merk op dat volgens het Europees Hof voor de Rechten van de Mens het ondervragingsrecht van (belastende) getuigen ook van toepassing is in civiele zaken: 'the requirement of fairness in Article 6 § 1 and the principle of equality of arms embody a right to examine

vullend onderzoek plaatsvindt om de inhoud van een anonieme melding te verifiëren. Ook in dit verband is een strakke proportionalisteitstoets, die we hierboven al aan de orde stelden, noodzakelijk.

In een klimaat waarin politiële databanken op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet (vgl. [7]), is het belangrijk om terughoudend te zijn met het voeden van politiële databanken met ongecontroleerde informatie. Dit pleit voor terughoudendheid bij het faciliteren van anonieme meldingen.

3.4 Publiek-private samenwerking

Stichting M. is een private partij die een rol vervult in de strafrechtspleging door meldingen van misdaad op te nemen, te filteren en door te geven aan de politie. Ook worden misdaadmeldingen doorgegeven aan andere partners, waaronder private partijen als energienetbeheerders en verzekeraars, die ook acties kunnen ondernemen op basis van de anonieme misdaadmeldingen.

Het toebedelen van taken aan private partijen in het kader van de strafrechtspleging, en breder in de veiligheidszorg, past in een tendens van toenemende publiek-private samenwerking (PPS). Het vervullen door private partijen van een bij uitstek van oudsher publieke taak vraagt om normatieve reflectie. Omdat de normatieve aspecten van een privaat Internetmeldpunt niet verschillen van die van het bestaande telefonische meldpunt, gaan we hier niet als zodanig op in. We verwijzen naar bestaande literatuur die een kader biedt voor reflectie.

Hoogenboom en Muller [16] bespreken vele perspectieven op publiek-private samenwerking in de veiligheidszorg, waaronder samenwerkingsverbanden waarbinnen strafrechtelijke informatie wordt gedeeld. Zij schetsen de ambivalentie van PPS-constructies, waarbij enerzijds het beleid veelal tamelijk kritiekloos en retorisch de rol van private partijen omarmt vanuit een gedeelde maatschappelijke verantwoordelijkheid voor veiligheid, en anderzijds in de beleidsdiscussie rechtsstatelijke bezwaren tegen PPS worden geformuleerd (zie Hoogenboom en Muller [16], met name hun bespreking van dogma 12: 'PPS is goed en moet (I)' en dogma 15: 'PPS is goed en moet (II)'). Van Steden [28] stelt in aansluiting hierop pertinente normatieve vragen, die beantwoord moeten worden in de beleidsafweging rond een anoniem Internetmeldpunt en het doorgeleiden van misdaadmeldingen aan private afnemers: 'Wat kunnen of gaan al die private partijen met unieke en vaak vertrouwelijke overheidsinformatie doen? Wie waarborgt de zekerheid dat die informatie voor het beoogde doel wordt gebruikt en aan wie moeten ze verantwoording afleggen?'

Aanknopingspunten voor het borgen van het publiek belang (waaronder ook de rechtsbescherming van individuen over wie anonieme meldingen worden gedaan) kunnen worden gevonden in het WRR-rapport *Het borgen van publiek belang*. Omdat organisaties vaak uit zichzelf niet uitsluitend oog hebben voor het publiek belang, moeten zij worden gedisciplineerd om de publieke belangenbehartiging veilig te stellen. Het rapport schetst vier mechanismen om het publiek belang te borgen:

- 'regels (vastgelegd in wetten of contracten);
- concurrentie (zowel concurrentie op als om de markt, bij uitbestedingen van taken);
- hiërarchie (de politieke bestuurder geeft aanwijzingen aan zijn ondergeschikten);
- institutionele waarden (versterking van de waarden en normen binnen een organisatie die de behartiging van het betreffende publieke belang ondersteunen).' [34, p. 10]

Aangezien in het onderhavige geval van een anoniem misdaadmeldpunt niet veel kan worden verwacht van concurrentie, noch van hiërarchie in de constructie van een private stichting en machtige private afnemers, zal bij de beleidsafweging rond een Internetmeldpunt vooral aandacht moeten worden besteed aan de borging van het publieke belang in contractuele regels en een wettelijke basis, en vooral in institutionele verankering van publieke waarden als rechtsbescherming, non-discriminatie, privacy en 'due process'. De overheid dient daarbij een strakke regie te voeren [34, p. 12].

witnesses against one in civil cases.' EHRM 26 maart 2002, B.H. t. Verenigd Koninkrijk, appl.nr. 59580/00. De reikwijdte van het ondervragingsrecht in civiele of bestuurlijke zaken is echter niet duidelijk, aangezien hier veel minder jurisprudentie over is dan in strafrechtzaken. Het gebruik van anonieme meldingen buiten de context van strafrechtelijke beslissingen roept daarom wezenlijke vragen op over de rechtsbescherming van degenen die belast worden in anonieme meldingen.

Hoofdstuk 4

Technische aspecten

In dit hoofdstuk gaan we in op de technische aspecten die van belang zijn bij Internetmelden. De inhoud van dit hoofdstuk is in ruwweg twee delen te splitsen. In het eerste deel behandelen we aandachtspunten en risico's in het algemeen, terwijl we in het tweede deel specifiek ingaan op een aantal mogelijke oplossingsrichtingen. De inhoud van dit hoofdstuk is gebaseerd op gesprekken met experts, analyse van bestaande systemen en interne brainstormsessies. Technische afkortingen worden verklaard in bijlage A.

4.1 Communicatie en anonimiteit

De vorm van communicatie over het Internet heeft invloed op de mate van anonimiteit. Figuur 4.1(b) geeft een abstracte weergave van de communicatie tussen de melder en het meldpunt via het Internet. Ter referentie is in figuur 4.1(a) het communicatiepad via de telefoon weergegeven. We onderscheiden vijf componenten: de melder, de ISP (Internet Service Provider) van de melder, het (tussenliggende) Internet, de ISP van het meldpunt en het meldpunt zelf. Het Internet fungeert hier als communicatienetwerk tussen de ISPs. Het precieze pad dat de data afleggen ligt van tevoren niet vast: afhankelijk van de aanwezigheid en drukte van de verbindingen wordt telkens geprobeerd de beste route voor de data te gebruiken. Elk van deze vijf componenten heeft andere risico's ten aanzien van de anonimiteit van de melder.

Bij anonieme communicatie tussen een melder en het meldpunt zijn twee aspecten van belang: de metadata (wie communiceert er met het meldpunt), en de inhoud (waarover wordt er gecommuniceerd). Het is van groot belang ook de inhoud te beschermen, omdat deze nog niet gefilterd is door een medewerker in het meldpunt. Het is dus zeer goed mogelijk dat de inhoud direct of indirect kan leiden tot de identificatie van de melder, net zoals metadata dat kunnen. In het huidige systeem met telefonische meldingen worden de metadata en de inhoud op de volgende manieren beschermd:

Metadata De weg die een gesprek aflegt is weergegeven in figuur 4.1(a). Op ieder van deze punten is metadata in principe beschikbaar. Echter, een verzameling van maatregelen maakt het zo lastig mogelijk om toegang te krijgen tot deze metadata:

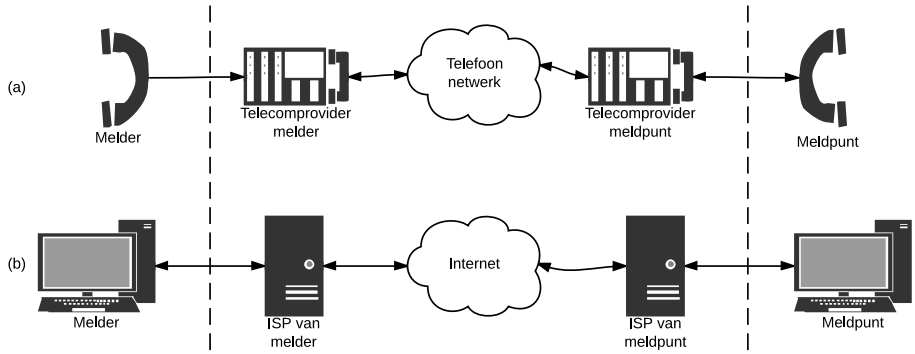
- de melder wordt aangespoord het telefoonnummer van het meldpunt uit zijn bellijst te verwijderen;
- de telecomproviders (van de melders) hebben toegezegd het telefoonnummer van het meldpunt niet op de rekening van de melder te zetten;
- het meldpunt ontvangt geen nummerweergave van zijn telecom provider; en
- een afspraak met het College van Procureurs-Generaal garandeert dat opsporingsdiensten slechts in uitzonderlijke gevallen de meta-informatie op mogen vragen bij de telecomproviders.[1]

Inhoud De inhoud van de conversatie wordt nergens fysiek opgeslagen (tenzij er een tap aanwezig is, zie paragraaf 5.3.1 voor de juridisch analyse hiervan). Deze kan immers identificerende informatie bevatten. Eventuele aantekeningen van de medewerkers van het meldpunt worden na afloop van de melding vernietigd.

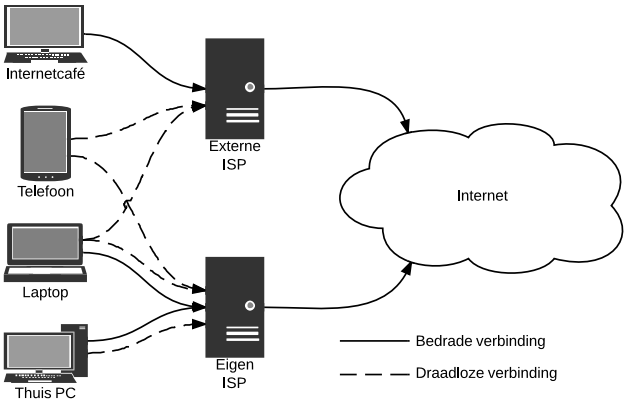
Ook een Internet-gebaseerde oplossing zal afdoende bescherming van zowel de metadata als de inhoud moeten bieden. In paragraaf 4.4 zullen we deze twee eigenschappen classificeren als respectievelijk *onobserveerbaarheid* en *confidentialiteit*.

Bovenstaande analyse voor het telefoonnetwerk illustreert de invloed die de vijf verschillende componenten in figuur 4.1(a) hebben op de anonimiteit van de oplossing. Dit geldt ook voor een Internet-oplossing. In paragraaf 4.6 zullen we de risico's analyseren die voortvloeien uit deze vijf elementen.

[1] De Wet bewaarplicht telecommunicatiegegevens bepaalt dat telecomproviders deze meta-informatie gedurende één jaar moeten bewaren, zie ook paragraaf 5.3.1.



Figuur 4.1: *Een overzicht van het communicatiekanaal tussen melder en meldpunt via (a) het telefoonnetwerk en (b) het Internet.*



Figuur 4.2: *Gedetailleerde weergave van het communicatiekanaal tussen de melder en het Internet. De externe ISP kan de ISP van het Internetcafé zijn, maar zal in veel gevallen een openbaar hotspot zijn in een trein, café of hotel.*

4.2 Infrastructuur

Voor de analyse van de risico's is de specifieke infrastructuur van de melder en het meldpunt van belang. De schets in figuur 4.1 is erg abstract. In de praktijk is de infrastructuur ingewikkelder, zowel aan de kant van de melder als aan de kant van het meldpunt. De melder kan met verschillende apparaten, via verschillende kanalen en via verschillende ISPs verbinding maken met het Internet, zie figuur 4.2. Ook voor het meldpunt is de situatie ingewikkelder, zie paragraaf 4.2.3.

4.2.1 Inrichting melder

Niet alle apparaten hoeven in eigendom te zijn van de melder, of volledig onder zijn beheer te vallen. In een Internetcafé heeft de melder noch de computer in eigendom noch heeft hij beheertoegang daartoe. Ook bij een laptop of vaste PC kan het voorkomen dat de melder geen beheertoegang heeft indien deze bijv. in bedrijfseigendom is. Dit betekent dat het installeren van software niet altijd mogelijk is, noch dat beveiligde verbindingen te vertrouwen zijn (zie paragraaf 4.6.2).

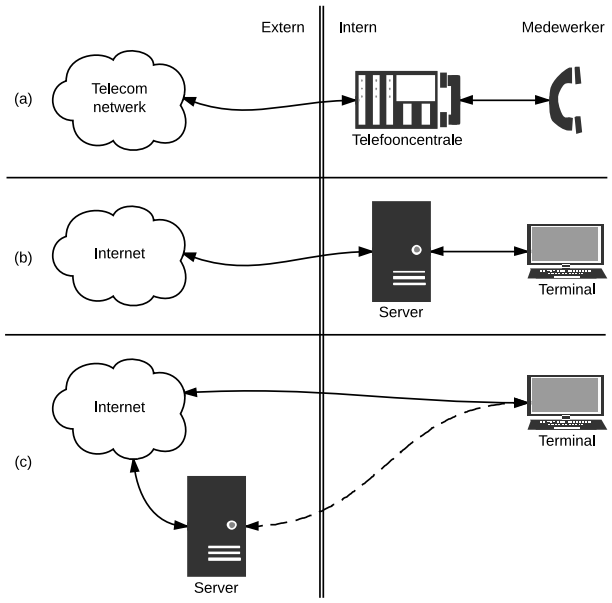
Naast het apparaat zelf is ook de verbinding tussen apparaat en ISP van belang. Een bedrade verbinding is redelijk veilig, maar een draadloze verbinding kan extra risico's met zich mee brengen. Dit geldt ook voor een externe ISP. Zie paragraaf 4.6 voor een meer gedetailleerde analyse. Tot slot kan de draadloze verbinding tussen de telefoon en de eigen ISP een WIFI verbinding zijn, maar ook een mobiele dataverbinding. In het laatste geval treedt de telecomprovider op als ISP.

4.2.2 VoIP

Als de melder de telefonische meldlijn belt via VoIP is er sprake van een hybride situatie. De melder maakt gebruik van zijn Internetverbinding als transportmedium om op deze manier zijn VoIP provider te bereiken. Deze zal uiteindelijk de telefoonverbinding die eerst over het Internet liep overzetten naar het traditionele telefonie netwerk. Op deze manier is een combinatie ontstaan van melden via telefonie en via het Internet.

Er zijn verschillende implementaties van VoIP mogelijk: (1) aangeboden door de eigen ISP met fysieke telefoon, (2) aangeboden door een externe partij met fysieke telefoon en (3) aangeboden door een externe partij via de computer (het veelgebruikte Skype valt in deze laatste categorie als het gebruikt wordt om met het bestaande telecomnetwerk te verbinden). Een uitgebreide risicoanalyse valt buiten scope van deze quickscan. Echter, de veiligheid van (1) en (2) zal niet veel verschillen van de bestaande telefonische situatie (mits (2) gebruikt maak van versleuteling). In geval (3) zijn in ieder geval alle risico's uit paragraaf 4.6.2 zonder meer van toepassing.[2] Tot slot, omdat het gesprek uiteindelijk via het

[2]Crimestoppers UK raadt het gebruik van Skype en andere VoIP oplossingen zelfs expliciet af, zie `https://crimestoppers-uk.org/most-wanted/how-to-give-information` bezocht op 26 februari 2014.



Figuur 4.3: *Overzicht van de infrastructuur bij het meldpunt met drie varianten: (a) de bestaande telecomsituatie; (b) een Internet-oplossing met een lokale server; en (c) een Internet-oplossing met een externe server (zie tekst voor nadere uitleg).*

telecomnetwerk verloopt is hierop dezelfde tap- en dataretentiewetgeving van toepassing die ook voor traditionele telefonie geldt.

4.2.3 Inrichting meldpunt

De interne netwerkarchitectuur van het meldpunt heeft grote invloed op de veiligheid van het meldpunt. Figuur 4.3 illustreert mogelijke situaties aan de kant van het meldpunt. Bij telefonische meldingen garandeert de opzet dat informatie uit een telefoongesprek nooit zomaar in een melding in het meldsysteem terechtkomt, aangezien een medewerker in het meldpunt bewust een rapport schrijft naar aanleiding van het gesprek.

Wij zijn van mening dat een dergelijke scheiding tussen binnenkomende informatie en uitgaande informatie ook in een Internet-gebaseerd systeem essentieel is. We gaan daarom uit van de volgende architectuur. In het meldpunt worden voor iedere medewerker twee systemen ingericht: (1) het systeem waarmee de medewerker met de melder communiceert (in figuur 4.3 is dit de terminal) en (2) een fysiek ander systeem waarin de medewerker uiteindelijk de melding invoert in het meldsysteem (dit is in figuur 4.3 niet weergegeven). Het eerste systeem moet zoveel mogelijk afgeschermd worden en alleen gebruikt worden voor communicatie met melders. In het bijzonder mag er geen verbinding mogelijk zijn tussen beide systemen. Op deze manier is het weer de medewerker die meldingen screent en overzet.

Voor iedere Internet-oplossing zal het meldpunt moeten voorzien in een server waar de communicatie met de melders in eerste instantie terechtkomt. De server vervult daarmee een soortgelijke rol als de telefooncentrale. De telefoon van de medewerker is vervangen door een terminal of computer die de communicatie met de melder weergeeft.

We maken onderscheid tussen een lokale server (figuur 4.3(b)) en een externe server (figuur 4.3(c)). Onder een externe server verstaan we zowel een server in een extern datacentrum als een server als onderdeel van een clouddienst. Als de server extern is ondergebracht moet de terminal verbinding maken met de server via het Internet. De conceptuele verbinding tussen de terminal en de server die zo ontstaat is gestreept weergegeven in figuur 4.3.

4.3 Communicatievorm van de melding

Er zijn verschillende manieren waarop een digitale melding binnen kan komen bij het meldpunt. Dit kan invloed hebben op de kwaliteit van de melding, maar ook op de daarbij behorende risico's. Hier bespreken we kort de verschillende vormen.

In de onderstaande classificatie spreken we over *sessies*. Een sessie is een aaneengesloten uitwisseling van berichten tussen melder en meldpunt die niet wordt onderbroken door een andere activiteit. Ter illustratie: het versturen van een brief is een sessie, het voeren van een telefoongesprek is dat ook.

De eerste classificatie behelst de interactiviteit van de sessie. In het geval van niet-interactieve sessies maken we nog een verder onderscheid tussen gestructureerde meldingen en ongestructureerde meldingen:

Interactief We noemen een sessie *interactief* als de melder en een medewerker bij het meldpunt in real-time met elkaar interacteren, d.w.z. meerdere berichten over een weer uit wisselen. Typische voorbeelden hiervan zijn een telefoongesprek of een chatgesprek.

Niet-interactief Een sessie is *niet-interactief* als de communicatie tussen de melder en het meldpunt slechts in één richting verloopt (van de melder naar het meldpunt, of van het meldpunt naar de melder). Typische voorbeelden hiervan zijn: het invullen en versturen van een formulier, het sturen van een brief en het sturen van een e-mail. Bij niet-interactieve sessies kunnen we de volgende twee situaties onderscheiden:

Gestructureerde meldingen De melder kan ondersteund worden door een intelligent formulier dat aangeeft welke informatie aan het meldpunt verstrekt moet worden en welke niet. Uitbreidingen hierop waarbij lokaal de invoer van de gebruiker gevalideerd wordt voordat die verstuurd wordt zijn ook denkbaar. Deze manier van melden kan relevant en nuttig zijn indien het type melding vooraf bekend is, bijvoorbeeld bij het melden van hennepteelt.

Ongestructureerde meldingen Aan de andere kant is het mogelijk de vereiste informatie niet gestructureerd uit te vragen. Dit is bijvoorbeeld het geval bij het versturen van een e-mail.

Een andere classificatie is hoe vaak er een sessie is tussen de melder en het meldpunt. Hierbij onderscheiden we eenmalige meldingen en meermalige meldingen. Dit onderscheid is belangrijk omdat bij een meermalige melding gevoelige informatie voor langere tijd bewaard moet worden.

Eenmalig Bij een *eenmalige* melding vind er slechts één sessie plaats tussen de melder en het meldpunt. Voorbeelden zijn een telefoongesprek, een chatgesprek of een enkele e-mail.

Meermalig Een melding kan ook *meermalig* zijn. In dat geval zijn er meerdere sessies tussen de melder en het meldpunt waarin de melder informatie aan het meldpunt kan verstrekken. Het meldpunt moet in dit geval een koppeling kunnen maken tussen deze sessies. We maken onderscheid tussen de volgende drie situaties:

Geen terugkoppeling Het meldpunt heeft geen mogelijkheid om berichten naar de melder te sturen.

Passieve terugkoppeling Bij passieve terugkoppeling kan het meldpunt (indien nodig) berichten achter laten voor de melder. Het is echter aan de melder om deze berichten te controleren en waar nodig meer informatie te verstrekken in een nieuwe sessie (bijv. door meer documenten te versturen, of een nieuwe interactieve sessie op te zetten).

Actieve terugkoppeling Bij actieve terugkoppeling kan het meldpunt zelf direct de melder bereiken. Een voorbeeld hiervan is het sturen van een antwoord op een e-mail van de melder of, in het telefonische geval, het terugbellen van de melder. Om dit te kunnen doen heeft het meldpunt dus contactgegevens van de melder nodig.

In de hedendaagse praktijk van stichting M. zijn de meldingen altijd telefonisch en worden ze afgerond binnen hetzelfde telefoon gesprek, waardoor deze meldingen altijd interactief en eenmalig zijn. Bij het melden via Internet zijn ook andere combinaties mogelijk, deze komen aan bod in paragraaf 4.8.

4.4 Criteria

We geven een aantal criteria aan de hand waarvan de kwaliteit van een technische oplossing getoetst kan worden. We zullen deze criteria gebruiken om een aantal mogelijke oplossingsrichtingen te scoren in paragraaf 4.8. De hier weergegeven criteria zijn het resultaat van gesprekken met experts en interne brainstormsessies.

Anonimiteit kan op twee conceptueel verschillende typen componenten geschonden worden. Ten eerste kunnen er in de eindpunten fouten gemaakt worden waardoor daar gedurende of na afloop van de melding de anonimiteit in gevaar kan komen. Ten tweede kan de anonimiteit geschonden worden op de verbinding tussen de melder en het meldpunt. We onderscheiden deze criteria.

Anonimiteit in de eindpunten De mate waarin de anonimiteit gewaarborgd kan worden in de eindpunten hangt af van de risico's die specifieke oplossingen daarin veroorzaken.

Anonimiteit m.b.t. de verbinding De volgende twee criteria samen bepalen in welke mate een gekozen oplossing anoniem is met betrekking tot de verbinding (zie het begin van dit hoofdstuk voor een gedetaileerde analyse).

Onobserveerbaarheid Een verbinding is onobserveerbaar als partijen niet kunnen detecteren of een melder met het meldpunt communiceert of gecommuniceerd heeft. Merk op dat het hier dus niet gaat om de inhoud van de communicatie, maar alleen om de metadata.

Confidentialiteit De verbinding is confidentieel als alleen de melder en het meldpunt kennis kunnen nemen van de inhoud van de communicatie.

Daarnaast zijn ook de volgende criteria van belang bij het toetsen van een oplossing.

Technische eenvoud De technische eenvoud verschilt per oplossing. Hoe complexer een oplossing des te meer punten er zijn waarop uiteindelijk de anonimiteit van de melder in gevaar kan komen. Een hoger technische complexiteit zal dus de anonimiteit in de eindpunten verminderen. De analyse van een aantal bestaande oplossingen (met name klok-

kenluider sites) heeft aangetoond dat er veel aandachtspunten zijn en dat het veilig inrichten van een oplossing soms ingewikkeld kan zijn, zelfs als de oplossing al bestaat.

Gebruiksgemak gebruiker Het gemak voor de gebruiker verschilt per oplossing. Lastigere oplossingen kunnen resulteren in slechtere adoptie van het meldpunt, of fouten die de anonimiteit reduceren. Als de gebruiker bijv. eerst nieuwe software moet installeren om veilig verbinding te maken met het meldpunt werpt dit ofwel een extra drempel op om een melding te doen ofwel een risico als ook een onveilige melding zonder de software gedaan kan worden.

Kwaliteit van de melding De te verwachten kwaliteit van de melding verschilt per oplossing. Dit criterium is van belang omdat de keuze voor een technische inrichting de kwaliteit zeer kan beïnvloeden. Zo zal een eenmalige niet-interactieve oplossing waarschijnlijk leiden tot kwalitatief slechtere meldingen omdat medewerkers in het meldpunt niet extra relevante informatie kunnen uitvragen.

4.5 Aanvallers en andere partijen

Risico's onstaan niet alleen door zwakheden in de technische inrichting maar ook door partijen die er belang bij hebben de anonimiteit van de melder of de melding te ondermijnen. In dit document houden we rekening met de volgende aanvallers (Engels: adversaries) van het systeem.

Omgeving De omgeving van de melder heeft van nature makkelijk toegang tot de apparatuur van de melder. Het is belangrijk dat het melden ook voor de omgeving verborgen blijft. Vooral als de melding iemand uit de omgeving betreft.

Externen Externe partijen kunnen om vele redenen proberen om de anonimiteit van het systeem te ondermijnen. 'Hackers' kunnen proberen om systemen binnen te dringen om zo de anonimiteit van één of meerdere melders te onthullen. Zowel ideële motieven als financiële motieven zijn mogelijk. Criminelen en criminele organisaties kunnen er belang bij hebben de anonimiteit van meldingen te ondermijnen als ze vermoeden dat ze regelmatig door anonieme meldingen worden dwarsgezeten (denk aan hennepkwekerijen). Ook andere 'slachtoffers' van anonieme meldingen, te denken valt aan fraudeurs, kunnen proberen om achter de identiteit van de melder te komen. Voor al deze partijen geldt dat ze kunnen proberen de indruk te wekken achter de identiteit van de melders te kunnen komen om zo potentiële melders af te schrikken.

Opsporingsdiensten Opsporingsdiensten kunnen achteraf verbindingsgegevens opvragen en communicatiekanalen tappen. Daarnaast kunnen ze grote belangen hebben bij het leren kennen van de identiteit van anonieme melders. We verwijzen naar paragraaf 5.3.1 voor een uitgebreidere juridische analyse.

De melder en het meldpunt spelen ook een rol. Ze kunnen een risico vormen voor de veiligheid en anonimiteit van het systeem.

Melder Als de melder de instructies niet opvolgt kan de melder zelf er voor zorgen dat zijn identiteit bekend wordt bij één van de andere partijen. In veel gevallen is er interventie van de melder nodig om te voorkomen dat er sporen aan zijn kant achterblijven. Bij het bellen naar het meldpunt is het bijvoorbeeld van belang om na afloop het telefoonnummer van het meldpunt uit de bellijst te halen.

Meldpunt Ook het meldpunt kan onzorgvuldig omgaan met de ontvangen informatie en zodoende de identiteit van de melder prijsgeven. In eerste instantie komt er heel veel informatie bijeen in het meldpunt. Als daar delen van achterblijven, bijvoorbeeld aantekeningen van een gesprek, kan dit leiden tot identificatie van de melder.

4.6 Algemene risico's

Hoewel er een aantal verschillende oplossingsrichtingen mogelijk zijn, zijn onafhankelijk daarvan een aantal risico's vrijwel altijd aanwezig. We zullen deze in een aantal groepen behandelen. Eerst behandelen we algemene risico's. De overige risico's groeperen we onder de relevante infrastructuurcomponenten. Indien mogelijk geven we een indicatie van de grootte van het risico.

4.6.1 Algemeen

We beginnen met een risico dat over de hele linie geldt.

Communicatie is vrijwel altijd observeerbaar. De communicatie tussen de melder en het meldpunt doorloopt alle vijf componenten die zijn aangegeven in figuur 4.1(b). Om deze communicatie mogelijk te maken weten alle tussenliggende partijen de herkomst en bestemming van een bericht. Als gevolg hiervan kunnen dus ook al deze partijen zien (als ze dat willen) wie er met het meldpunt communiceert.

De standaard manier om dit te voorkomen is door Tor[3]—een anonimiseringssysteem—te gebruiken. Tor zorgt er voor dat de partijen aan de kant van de melder niet zien met wie de melder communiceert en partijen aan de kant van het meldpunt, inclusief het meldpunt zelf, niet kunnen zien wie met het meldpunt communiceert. Echter, voor een normale gebruiker is het niet eenvoudig om Tor correct op te zetten en te gebruiken. Daarnaast is de aanwezigheid en het gebruik van Tor op zichzelf mogelijk verdacht.

In de traditionele telecomwereld is dit risico minder groot. Er spelen minder partijen mee—met wie je dus afspraken kan maken—en de infrastructuur is minder toegankelijk dan bij het Internet.

4.6.2 Risico's aan de kant van de melder

We bekijken nu de risico's aan de kant van de melder.

Onzorgvuldigheid melder. Veel van de oplossingen vereisen enige zorgvuldigheid van de gebruiker die verder gaat dan het wissen van een telefoonnummer achteraf. Soms moet alleen informatie achteraf verwijderd worden, bijvoorbeeld het weggooien van een melding uit de verzendbox van de e-mailclient, maar veelal is het ook sterk aan te raden vooraf maatregelen te nemen, door bijvoorbeeld de browser in private modus op te starten. De browser zal dan proberen om, na het sluiten van het venster, geen sporen achter te laten op de computer die informatie geven over de bezochte websites. Hieronder vallen in ieder geval tijdelijke bestanden, cookies en de surfgeschiedenis.

Sporen zijn voor de gebruiker niet goed te overzien. De informatie die wordt opgeslagen is niet goed te overzien voor een reguliere gebruiker van het systeem. Zo vormen o.a. de surfgeschiedenis, eventuele cookies en tijdelijk bewaarde afbeeldingen allemaal indicatoren dat de melder op de website van het meldpunt is geweest. Het verwijderen van deze informatie biedt geen garantie dat deze niet toch nog teruggehaald kan worden van bijvoorbeeld de harde schijf. Ook het gebruiken van private modus van de browser helpt niet tegen eerder al geplaatste informatie (bijvoorbeeld toen de melder las op de website van het meldpunt dat hij beter private modus kon gebruiken).

Systeem van melder is kwetsbaar. Met name als de melder een computer gebruikt is deze kwetsbaar voor allerhande malware, waaronder virussen en keyloggers. Als deze software aanwezig is is het voor kwaadwillenden relatief eenvoudig om de communicatie met het meldpunt te detecteren of af te luisteren. Dit risico is iets minder groot op mobiele platformen zoals Android en iOS.

Hoewel veel computers besmet zijn met malware, is het verwachte risico hiervan m.b.t. de anonimiteit niet heel groot. De partijen die de malware beheren zijn weliswaar op jacht naar persoonsgegevens, maar zullen in het algemeen geen belang hebben bij het achterhalen van de identiteit van de anonieme melder. Dit is uiteraard anders wanneer de aanvaller gericht het systeem van de melder besmet.

Melding over lokale partij. Iedereen die toegang heeft tot het lokale netwerk of de machine van de melder kan in principe alle communicatie zien, zie ook het vorige punt. Normaal gesproken is dit risico niet zo groot. Dit is echter anders als de melding iemand uit de directe omgeving betreft (bijv. bij een melding over een partner of werkgever).

In het bijzonder kunnen in dit geval niet alleen alle verbindingsgegevens worden opgeslagen, maar zelfs eventuele versleutelde verbindingen zijn niet meer veilig.[4] Het is dus belangrijk dat de persoon over wie de melding gaat geen toegang heeft tot de machine en het lokale netwerk van de melder.

4.6.3 Risico's Internetverbinding en ISPs

De ISP die door de melder wordt gebruikt vormt de toegangspoort tot het Internet. Al het verkeer tussen melder en meldpunt loopt dus ook hier langs. Dit brengt de volgende risico's met zich mee.

Onbeveiligde draadloze netwerken. Het is mogelijk dat de melder gebruikt maakt van een openbaar draadloos netwerk, zie figuur 4.2. In vrijwel alle gevallen is deze verbinding om praktische redenen niet versleuteld. Ook privénetwerken zijn soms slecht geconfigureerd waardoor deze effectief onbeveiligd zijn. Dit betekent dat eventuele aanvallers in de buurt van de melder de communicatie kunnen observeren.

We merken op dat zelfs als de communicatie zelf versleuteld is, de aanvaller in ieder geval kan zien met wie de melder communiceert, en dus bijvoorbeeld kan zien dat de melder de website van het meldpunt bezoekt.

Een melder kan zich beschermen tegen dit soort aanvallen door gebruik te maken van goed geconfigureerde VPN-verbinding, maar dit verhoogt de complexiteit van de oplossing. Het is lastig uit te leggen dat een VPN-verbinding nodig is om te zorgen voor een

[3] `https://www.torproject.org/`

[4] Het is mogelijk deze bescherming te omzeilen als je beheertoegang hebt tot de computer.

veilige verbinding. Ook moet de VPN-provider zelf nu vertrouwd worden.

Externe ISPs zijn niet altijd betrouwbaar. Externe ISPs leveren veelal een gratis dienst[5]; denk aan de Internetverbinding in een café, in de trein, op een station of luchthaven. Om aansprakelijkheid te beperken kan de ISP bijhouden wie waarmee verbinding heeft gemaakt. Daarnaast kan de gekozen technische oplossing soms (bijvoorbeeld in het geval van transparante proxies, die bezochte pagina's tijdelijk opslaan om ze sneller te kunnen leveren, of bewerken om reclame toe te voegen) er voor zorgen dat al dan niet opzettelijk verbindingsinformatie wordt opgeslagen.

Tot slot zou de ISP er voor kunnen kiezen om geld te verdienen door het surfgedrag van de gebruiker te verkopen en/of advertenties te plaatsen naar aanleiding van het surfgedrag van de gebruiker. In dit geval krijgen externe derde partijen informatie over het surfgedrag van de eventuele melder.

Als deze verbindingsinformatie gecombineerd wordt met andere gegevens over de gebruiker van het netwerk is het zeker mogelijk dat de identiteit van de melder achterhaald kan worden door (partners van) de externe ISP. De inhoud van de bijbehorende melding zal echter in de meeste gevallen niet achterhaald kunnen worden.

Aanvallen op de eigen ISP. Al het verkeer van de melder loopt via de ISP van de melder. Het verkeer kan hier dus goed afgeluisterd worden (zoals bijvoorbeeld gebeurt als er een IP-tap is geplaatst). Echter, reguliere ISPs zijn in de regel goed beveiligd. Dit geldt niet automatisch voor externe ISPs, zie ook de vorige paragraaf, deze zullen juist vaak minder goed beveiligd zijn, maar nog steeds beter dan de machine van de melder. Externe aanvallers zullen niet zomaar een ISP binnendringen om verkeer af te luisteren. Als het doel is de melder aan te vallen is het veel effectiever de computer van de melder zelf aan te vallen. Vergelijk ook met paragraaf 4.6.4 en met name paragraaf 4.6.5. Dit risico is dus klein.

4.6.4 Risico's op het Internet

De communicatie tussen melder en meldpunt gaat, nadat het de ISP van de melder is gepasseerd, het Internet op. In de weergave van figuur 4.1 bestaat het Internet uit een netwerk van computersystemen waarbinnen ieder paar computersytemen met elkaar kan communiceren. In de regel zijn dit ISPs of andere grote partijen. Strikt genomen maakt iedere machine met een Internetverbinding onderdeel uit van het Internet, maar voor deze discussie beschouwen we alleen die computersystemen die actief communicatie doorgeven.

De route die de communicatie aflegt hangt af van de herkomst en bestemming van de communicatie, de verbindingen in het netwerk en de drukte op het netwerk. Het is daarmee niet van te voren te zeggen welke route de communicatie af zal leggen. Systemen op de route zien de herkomst en bestemming van de communicatie, maar zullen deze, gezien de hoeveelheid data, nooit zomaar opslaan.

We verwachten niet een groot risico van aanvallen op het Internet zelf. De route is onvoorspelbaar, dus om een substantieel effect te bereiken moet op vrijwel ieder mogelijk pad een machine aangevallen zijn. Daarnaast zijn deze machines vrijwel altijd goed beveiligd. De meeste aanvallers zullen dit niet kunnen (met de mogelijke uitzondering van de veiligheidsdiensten). Voor alle aanvallers geldt (als ze tenminste het meldpunt zelf gericht aanvallen) dat ze de weg van de minste weerstand zullen kiezen. Het is veel effectiever de ISP van de melder (zie paragraaf 4.6.3) dan wel het meldpunt (zie paragraaf 4.6.5) af te luisteren om zodoende al het verkeer te kunnen onderscheppen.

4.6.5 Risico's bij ISP meldpunt

Zoals de ISP van de melder het verzamelpunt is van al het verkeer van en naar de melder (vergelijk paragraaf 4.6.3), zo is de ISP van het meldpunt het verzamelpunt van al het verkeer van en naar het meldpunt. Al dit verkeer kan hier dus afgeluisterd worden.

In de regel zal de ISP goed beveiligd zijn en deze informatie niet zomaar vrijgeven. Echter, waar het misschien niet interessant is een ISP van een melder aan te vallen kan het wel degelijk interessant zijn voor externe aanvallers om de ISP van het meldpunt aan te vallen en zo achter veel vertrouwelijke informatie te komen. Daarnaast zal de server van het meldpunt zelf (hopelijk) beter beschermd zijn tegen externe aanvallen dan bijvoorbeeld de machine van de melder. Hierdoor kan het opeens interessanter zijn om de ISP van het meldpunt aan te vallen dan de server van het meldpunt. Tot slot, hoewel de opsporingsdiensten in theorie een tap kunnen aanvragen op de verbinding tussen de ISP en meldpunt, zijn ze in juridische zin beperkt, zie paragraaf 5.3.1.

In het algemeen geldt dat het risico op het aanvallen van de ISP sterk verminderd kan worden door alle com-

[5] Merk op dat we hier de aanbieder van bijv. het gratis draadloze netwerk als ISP beschouwen. Juridisch gesproken zijn deze aanbieders overigens geen aanbieders van openbare electronische communicatiediensten en zij vallen dus niet onder de Telecommunicatiewet. In plaats daarvan geeft de dienstaanbieder de gebruiker slechts toegang tot zijn randapparatuur.

municatie te versleutelen. De communicatie is dan nog wel observeerbaar, d.w.z. bij de ISP is het zichtbaar wie met het meldpunt communiceert, maar wel confidentieel, d.w.z. de inhoud van de communicatie is niet te zien.

4.6.6 Risico's van het meldpunt

Het meldpunt vormt het eindpunt van alle communicatie met de buitenwereld; eventueel wordt deze communicatie intern nog verder geleid. Dit maakt in het bijzonder de server van het meldpunt erg kwetsbaar. Alle communicatie is hier in ruwe ongecensureerde vorm aanwezig en de eventueel versleutelde data wordt hier normaal gesproken ontsleuteld. Tot slot zal de server, in tegenstelling tot de telefooncentrale waar nummerweergave al was uitgeschakeld, vrijwel altijd zien wie verbinding maakt met het meldpunt.[6] Dit resulteert in de volgende risico's.

Computers zijn niet geheugenloos. Bij het melden via een telefoon is er een een-op-een overdracht van gesproken informatie naar de medewerker van het meldpunt. Het gesprek wordt niet opgenomen, behalve in het uitzonderlijke geval dat er een tap aanwezig is, en derhalve is de originele inhoud van het telefoongesprek niet te achterhalen (m.u.v. wat de medewerker onthoudt). Ook bij VoIP wordt de inhoud van het gesprek in principe[7] niet bewaard. Het voordeel hiervan is dat eventuele versprekingen van de melder die kunnen leiden tot zijn/haar identificatie niet te achterhalen zijn. Dit is *niet* het geval voor een digitale oplossing.

Ontvangen berichten, in welke vorm dan ook, moeten tijdelijk bewaard worden om ze weer te kunnen geven op het scherm van de medewerker bij het meldpunt. De architectuur van het systeem moet er op gericht zijn dat dergelijke informatie niet achteraf te achterhalen is. Dit is technisch mogelijk, maar vereist een zeer zorgvuldig ontwerp. Het ontwerp wordt eenvoudiger als enig informatieverlies acceptabel is (net zoals dat gebeurt wanneer een telefoongesprek halverwege verbroken wordt), bijvoorbeeld door de informatie slechts tijdelijk op te slaan in het werkgeheugen van de computer.

Langere opslag is lastig. Als meldingen niet-interactief zijn (denk hierbij aan e-mails, ingevulde webformulieren en toegevoegde documenten) moeten deze voor langere tijd bewaard worden totdat ze verwerkt kunnen worden door een medewerker. Dit geldt ook voor meermalige meldingen waar het systeem een koppeling tussen meldingen (voor meermalige meldingen zonder terugkoppeling en met passieve terugkoppeling), dan wel een koppeling tussen melder en melding (voor meermalige meldingen met actieve terugkoppeling) moet bijhouden.

Na het verwerken van de melding moet al deze informatie veilig verwijderd worden uit de systemen van het meldpunt. Aan de andere kant mag een melding niet zomaar verloren gaan.[8] In dit laatste opzicht verschilt dit risico van het hierboven genoemde risico: bij interactieve communicatie is informatieverlies mogelijk acceptabel; bij niet-interactieve communicatie en meermalige communicatie niet, omdat dit leidt tot een (voor de melder) ondetecteerbaar verlies van meldingen.

Documenten niet ontdaan van metadata. Indien het mogelijk is documenten (we verstaan hieronder alle typen bestanden waaronder foto's) te versturen naar het meldpunt—Stichting M. gaf eerder aan daar op dit moment het belang niet van in te zien—dan brengt dit extra risico's met zich mee. Allereerst is het voorgaande risico van toepassing op het langer bewaren van meldingen. Daarnaast kunnen ingestuurde bestanden metadata, zoals de auteur, datum en machine waarop het document gemaakt is, bevatten die de verzender kan identificeren (zelfs als de inhoud van de bestanden zelf daar niet voor zorgt).

Er bestaat software, zoals MAT[9] (Metadata Anonymisation Toolkit), die gebruikt kan worden om metadata te verwijderen. Echter, dergelijke software ondersteunt niet altijd alle mogelijke bestandsformaten en bepaalde metadata—zoals watermerken—zijn lastig te verwijderen [33].

Terminals in het meldpunt zijn kwetsbaar. Informatie over meldingen is in ieder geval voor enige tijd beschikbaar op de systemen van het meldpunt. Daarmee zijn deze systeem ook kwetsbaar voor gerichte aanvallen van buitenaf en besmetting met malware. In tegenstelling tot de eventuele fysieke aanvallen, zoals afluisteren met richtmicrofoons en liplezen, die mogelijk zijn bij telefoonsystemen zijn deze aanvallen ook mogelijk van grotere afstand. Daarnaast is het lastiger om je er tegen te beschermen.

Dit risico is te verminderen door de systemen in het meldpunt strikt te scheiden, zie de architectuurschets in paragraaf 4.2.3, zodat de terminals nooit direct van buitenaf bereikbaar zijn. Door de terminals voor één

[6] Overigens is het technisch mogelijk dat de ISP, als die hieraan meewerkt, de herkomst van het verkeer verbergt voor het meldpunt, net zoals thuisrouters verbergen dat er binnenshuis meerdere machines gebruik maken van het Internet in plaats van één.

[7] Tenzij de VoIP-aanbieder dat doet, maar dat ligt niet voor de hand.

[8] Voor de technici: opslag in het werkgeheugen voldoet dus niet.

[9] `https://mat.boum.org/`, bezocht op 5 januari 2014

heel specifiek doel in te richten is het makkelijker ze veilig te houden.

Fysieke toegang tot de server. De server van het meldpunt waarop de meldingen binnenkomen is kwetsbaar en bevat veel informatie.[10] Iedereen die fysiek toegang heeft tot de server kan redelijk makkelijk nieuwe communicatie afluisteren. Merk op dat gezien de locatie van de aanval de versleuteling van de data al verbroken is. Het is dus belangrijk om de server fysiek goed te beschermen.

Indien de server buiten de muren van het meldpunt geplaatst wordt (zie figuur 4.3c), en zich bijvoorbeeld in een extern datacenter of in de cloud bevindt, hebben meer partijen toegang tot de server. Aan de andere kant is de beveiliging in een datacenter misschien wel beter dan de beveiliging die in het meldpunt bereikt kan worden, bijvoorbeeld omdat er een sterkere nadruk is op fysieke beveiliging. Daarnaast heeft ook de specifieke inrichting van het beheer van een lokaal datacentrum invloed op de veiligheid (zie hoofdstuk 6).

4.7 Bestaande anonieme meldsystemen

Ter ondersteuning van onze analyse van mogelijke technische oplossingsrichtingen geven we een korte schets van een aantal bestaande oplossingen.

4.7.1 Crime Stoppers International

Stichting M. is aangesloten bij de internationale organisatie Crime Stoppers International.[11] Met name in de Angelsaksische landen zijn veel zusterorganisaties van Stichting M. actief. Echter, waar Stichting M. heel Nederland bestrijkt bedienen veel van deze zusterorganisaties een veel kleinere regio. Het is dan ook onmogelijk om een enigszins representatief overzicht te geven van deze verschillende organisaties.

Hoewel er veel verschillende organisaties zijn, lijkt het erop dat veel van deze gebruik maken van de TipSoft software.[12] De volgende twee pakketten zijn relevant voor dit onderzoek:

TipSoft WebTips Het TipSoft WebTips platform [31] is een website waarop melders met behulp van een gestructureerd formulier een melding kunnen doorgeven. De verbinding met de TipSoft organisatie is versleuteld. Daarnaast geeft TipSoft aan dat dit platform sinds kort interactieve chat tussen de melder en het meldpunt ondersteunt.

TipSubmit Mobile Het TipSubmit Mobile pakket [30] levert applicaties voor mobiele platformen (zowel Android als iOS) waarmee melders meldingen kunnen versturen naar het meldpunt. Deze applicaties leveren in eerste instantie een gestructureerd formulier, maar na het invullen hiervan is het ook mogelijk om een interactieve chat met het meldpunt te starten. Indien gewenst kan de melder beeldmateriaal uploaden naar het meldpunt.

In beide gevallen geldt dat alle data die door de melder worden doorgegeven aan het meldpunt (waaronder logs van de gesprekken, ingevulde formulieren en foto's) daar letterlijk worden opgeslagen en later in te zien zijn. Dit is risicovol aangezien deze data nog niet geanonimiseerd zijn, zie ook paragraaf 4.6.6. Daarnaast bewaart de mobiele applicatie de inhoud van de meldingen, waardoor deze later bij de melder te herkennen zijn en dus een risico vormen voor de melder, zie ook paragraaf 4.6.2. We constateren dat beide systemen de nadruk leggen op gebruikersgemak, en nauwelijks aandacht besteden aan de bescherming van de anonimiteit.

Ook veel overheden richten tegenwoordig anonieme meldpunten in voor het melden van bijvoorbeeld terrorisme en belastingfraude. De precieze werking hiervan valt buiten het bereik van dit onderzoek.

4.7.2 Klokkenluiderssites

Een duidelijk andere categorie wordt gevormd door klokkenluiderssites. Hier wordt veelal uitgegaan van veel krachtigere aanvallers (bijvoorbeeld van het kaliber inlichtingendiensten) en de beveiligingsmaatregelen zijn dan ook navenant groter.

Voor dit onderzoek hebben we kort gekeken naar SecureDrop[13], Zeit Briefkasten[14], en GlobaLeaks[15]. In alle gevallen is er door de makers veel moeite gedaan om de oplossingen zo anoniem mogelijk te maken. Zo zijn SecureDrop en GlobaLeaks alleen via Tor te bereiken en moet er een apart werkstation ingericht worden om documenten veilig in te zien. De ontwerpdocumenten [1, 13, 20, 27] en de beveiligingsanalyses [10, 14] illustreren de complexiteit van dergelijke oplossingen.

[10] De server die de uiteindelijk door de medewerker opgemaakte meldingen verwerkt bevat alleen geanonimiseerde meldingen en is, net als in de telefonische situatie, alleen een risico voor de persoon waarover gemeld is, niet voor de melder zelf.

[11] `www.csiworld.com` bezocht op 26 februari 2014.

[12] `http://www.tipsoft.com/`, bezocht op 26 februari 2014.

[13] `https://pressfreedomfoundation.org/securedrop`, voorheen DeadDrop en door The New Yorker gebruikt onder de noemer Strongbox.

[14] `http://www.zeit.de/briefkasten/index.html`, aangeboden door het Duitse nieuwsblad Zeit.

[15] `https://globaleaks.org/`, onder ander gebruikt door `publeaks.nl`.

4.8 Mogelijke technische inrichtingen

In deze paragraaf schetsen we een aantal mogelijke technische oplossingen. Deze oplossingsrichtingen zijn voortgekomen uit gesprekken met experts, interne brainstormsessies en een analyse van bestaande systemen. Het doel is uitdrukkelijk niet om een uitputtend overzicht te genereren. We geven een korte analyse van deze oplossingen in termen van voor- en nadelen.

4.8.1 Web

Veel van de bestaande oplossingen (zie paragraaf 4.7) zijn gebaseerd op webpagina's. In dit geval biedt het meldpunt een webpagina aan waarmee gebruikers een melding kunnen doen. Webpagina's zijn tegenwoordig erg flexibel (het zijn bijna volwaardige programma's die binnen de browser draaien) en bieden daarmee vele mogelijkheden voor interactieve meldingen, maar ook voor niet-interactieve gestructureerde meldingen met uitgebreide vragenlijsten. Juist omdat de mogelijkheden zo divers zijn zullen we een aantal kort verder uitwerken.

Er bestaan goede standaarden voor het versleutelen van webverkeer (SSL/TLS). We gaan er dan ook vanuit dat alle oplossingen alleen via een versleutelde verbinding te benaderen zijn. Ook aan de client kant is er de laatste jaren veel vooruitgang geboekt. Alle browsers bieden tegenwoordig een incognito of private modus aan, zodat het aannemelijk is dat er weinig tot geen sporen op het systeem van de melder achterblijven.

Voordelen:

- Een website is een concept waar de melder al mee bekend is. De melder hoeft zich niet te bekwamen met een volledig nieuw systeem.
- De melder kan gebruik maken van iedere computer met Internet. Systemen in publieke ruimten (Internetcafé, bibliotheek, etc.) zijn dus ook te gebruiken.

Nadelen:

- Het aanbieden van een website behelst een complexe combinatie van verschillende elementen die allemaal correct geconfigureerd moeten worden. Met name webservers zijn dusdanig ingewikkeld dat vergaande kennis van het systeem vereist is om zowel directe als indirecte opslag van verkeersgegevens uit te schakelen.
- De veiligheid van een versleutelde verbinding staat en valt met de controle van de melder. De melder moet zelf controleren of de versleuteling in orde is *en* of de partij waarmee hij communiceert ook echt het meldpunt is. Dit vereist enige technische kennis. Vooral omdat juist in het geval van een aanval eventuele informatie hierover op de pagina's van het meldpunt uiteraard ook vervalst wordt.

Webgebaseerd formulier

De oplossing die door veel buitenlandse meldpunten wordt aangeboden is een webformulier (zie paragraaf 4.7). De melder beantwoordt een aantal vragen—en is er vaak zelf voor verantwoordelijk geen identificerende informatie achter te laten.

Een oplossing met een formulier is vrijwel altijd eenmalig en niet-interactief (zie de webgebaseerde berichtenbox hieronder voor een meermalige oplossing), maar het kan zowel gestructureerd als ongestructureerd zijn.

Voordelen:

- Een van de eenvoudigste websystemen om op te zetten.

Nadelen:

- Het systeem is eenmalig en niet-interactief. De verwachte kwaliteit van de meldingen is daarmee lager dan wanneer interactie wel mogelijk is.

Webgebaseerd chatten

Een oplossing die wordt aangeboden door een aantal online hulpdiensten, waaronder het meldpunt kinderporno[16], is een online chatdienst (deze diensten zijn webgebaseerd, voor 'echte' chatdiensten via bestaande chat-oplossingen verwijzen we naar paragraaf 4.8.3). Ook voor een anoniem meldpunt kan een dergelijke dienst ingericht worden. Melders chatten dan met een medewerker van het meldpunt.

Deze oplossing is interactief en normaal gesproken eenmalig (hoewel meermalige oplossingen altijd denkbaar zijn).

Voordelen:

- Door de interactiviteit van de oplossing is de kwaliteit van de melding waarschijnlijk hoger dan die van niet-interactieve oplossingen.

Nadelen:

- Volwassenen typen, naar ervaring van de experts uit de expertmeeting, te langzaam voor een dergelijke dienst.

[16] `http://www.meldpunt-kinderporno.nl/`

Webgebaseerde berichtenbox

De laatste mogelijkheid is een webgebaseerde berichtenbox. Bij de bestaande oplossingen worden deze vaak gebruikt voor zogenaamde klokkenluiderssites (zie paragraaf 4.7). Klokkenluiders kunnen hier berichten en documenten achter laten. Vaak is een voorziening getroffen om later nog vragen te stellen aan de klokkenluider (klokkenluiders ontvangen hiertoe een speciale code waarmee ze zich later opnieuw bij het meldpunt kunnen identificeren). Echter, de klokkenluider moet altijd zelf het initiatief nemen opnieuw in te loggen en deze berichten ook daadwerkelijk te bekijken. Dit geldt ook voor de TipSoft WebTips-oplossing. Deze systemen zijn niet-interactief, meermalig en met passieve terugkoppelmogelijkheid.

Het grote verschil met de formulieroplossing hierboven is dus de mogelijkheid tot het doen van een meermalige melding. Hiertoe ontvangt de melder een speciale code, waarmee hij zich later nogmaals bij het meldpunt kan identificeren.

Voordelen:

- Er is al expertise op dit gebied en de software verkrijgbaar (in het geval van de klokkenluiderssites zelf vrij beschikbaar).
- Doordat de meldingen meermalig zijn wordt een functionaliteit mogelijk die lijkt op die van een interactieve melding. Deze mogelijkheid is wel beperkt. Ten eerste is de terugkoppeling passief: de melder zal zelf het initiatief moeten nemen om te controleren of er berichten voor hem zijn achter gelaten. Ten tweede zal het in het algemeen lang duren (langer dan bij bijv. chatten) voordat het meldpunt een reactie ontvangt van de melder.

Nadelen:

- De oplossing is technisch complex.
- Doordat meldingen meermalig zijn is de afhandeling ervan door het meldpunt een stuk lastiger.
- De speciale code moet veilig bewaard worden door de melder. Ten eerste is deze code nodig om later meer informatie aan het meldpunt te verstrekken, en ten tweede is het in je bezit hebben van de code op zichzelf een risico.
- Hoewel de functionaliteit aanwezig is die lijkt op die van een interactieve melding levert echte interactie (binnen één sessie) waarschijnlijk een hogere kwaliteit.

4.8.2 E-mail

Het meldpunt kan een eenvoudige oplossing realiseren door een e-mailadres te publiceren dat beheerd wordt door het meldpunt. Melders sturen simpelweg een e-mail met de volgens hun relevante informatie. Een e-mail bevat standaard, meer dan de andere oplossingen, allerlei metadata. Het is daarom belangrijk dat de ontvangende mailserver aan de kant van het meldpunt al deze data direct verwijdert.

E-mail biedt normaal gesproken geen confidentialiteit van de verbinding. Een manier om dit op te lossen is door gebruik te maken van versleuteling met bijvoorbeeld PGP. Er zijn reguliere oplossingen beschikbaar voor de verschillende besturingssystemen. Daarnaast kan PGP eventueel—de veiligheidsimplicaties hiervan zijn niet te analyseren binnen deze quickscan—in een webbrowser worden geïntegreerd.[17] In alle gevallen dient het meldpunt een publieke sleutel beschikbaar te stellen, zodat melders meldingen kunnen versleutelen voor ontsleuteling door de juiste ontvanger.

Er is een onderscheid te maken tussen een lokale e-mailclient (deze zal vrijwel altijd gekoppeld zijn aan het e-mailadres van de melder) en een online webmailclient (hier kan de melder er voor kiezen om een nieuw anoniem e-mailadres aan te maken). In het tweede geval is het gebruik van PGP wel een stuk lastiger.

Een e-mailoplossing is niet-interactief. Ze kan eenmalig of meermalig (met eventueel actieve terugkoppeling) zijn afhankelijk van de inrichting.

Voordelen:

- De melder kan een online webmailclient met een speciaal nieuw e-mailadres gebruiken voor extra anonimiteit. In dit geval is zelfs meermalige communicatie met terugkoppeling mogelijk zodat de oplossing bijna interactief is.
- Als er geen versleuteling gebruikt wordt is dit een eenvoudig te begrijpen concept.
- Als er correcte versleuteling (d.w.z. met een veilig algoritme en voldoende lange sleutels) gebruikt wordt is de confidentialiteit van de berichten gegarandeerd.

Nadelen:

- Als er geen versleuteling gebruikt wordt is de inhoud voor iedere tussenliggende mailserver leesbaar.
- Voor het installeren van versleutelsoftware is beheertoegang nodig tot de machine.
- Als wel versleuteling gebruikt wordt is er een groot risico op misconfiguratie van de PGP-client dan wel het versturen van onversleutelde e-mail.
- Als er meermalige communicatie met terugkoppeling plaats vindt moet ook de melder een sleutelpaar genereren, wat op zich weer risico op iden-

[17] bijv. WebPG, `https://webpg.org`

tificeerbaarheid en misconfiguratie met zich mee brengt.
- Als versleuteling gebruikt wordt kan de aanwezigheid van de daartoe te gebruiken software een hint zijn voor de omgeving dat een melding is gedaan.
- Als versleuteling wordt gebruikt kan de aanwezigheid van een sleutelpaar voor het meldpunt een duidelijke aanwijzing zijn voor het doen van een melding.

4.8.3 Chat

Het gaat hier om het gebruiken van bestaande chat-oplossingen (zoals bijvoorbeeld Google Talk, IRC, Skype, en Jabber). Een website die een directe chat-functionaliteit biedt met het meldpunt valt onder paragraaf 4.8.1. De gebruiker maakt gebruik van zijn bestaande chat-oplossing, en communiceert daarmee met het meldpunt dat een chat-account publiek beschikbaar heeft gemaakt.

Het meldpunt zorgt er voor dat lokaal geen logs opgeslagen worden van de chat-sessies en dat na afloop alle contactgegevens verwijderd worden. Als de melder een nieuw chat-account aanmaakt (vergelijkbaar met een nieuw e-mailaccount) kan de het meldpunt later opnieuw contact opnemen met de melder. Een chat-oplossing is daarmee interactief, meermalig en met actieve terugkoppeling.

Voordelen:

- Deze oplossing is interactief, met als gevolg waarschijnlijk een melding van hogere kwaliteit.
- De gebruiker kan gebruik maken van zijn bestaande chat-oplossing.
- Het is waarschijnlijk makkelijker een initiële oplossing op te zetten.

Nadelen:

- Vrijwel altijd is het nodig een apparaat van de melder te gebruiken. Publieke systemen staan installatie van chatclients vaak niet toe.
- De communicatie verloopt via andere servers. In de meeste chatprotocollen betekent dit dat de communicatie via één of meerdere (de)centrale servers verloopt die niet allen onder het beheer van de stichting vallen. (Meta-)informatie kan hier dus achterblijven, geanalyseerd en eventueel opgevraagd worden.
- De communicatie is niet altijd/overal versleuteld. Afhankelijk van het protocol is de communicatie niet versleuteld, of kan die op z'n minst op een centrale server gelezen worden. Dit risico is af te vangen door het gebruik van een oplossing als Off-the-Record (OTR) Messaging [15] die end-to-end encryptie garandeert. Dit maakt het gebruik echter wel veel ingewikkelder, met name omdat niet alle clients OTR ondersteunen en/of dit standaard aanbieden.
- Vrijwel alle chatapplicaties slaan de gevoerde gesprekken op. Na het doen van een melding moet de melder deze opgeslagen gesprekken verwijderen. Ook moet het meldpunt weer uit de contactenlijst verwijderd worden.
- Afhankelijk van het chatprotocol heeft het meldpunt veel tot weinig controle over welke informatie op de server achterblijft—met name informatie die de melder kan identificeren is extra kwetsbaar.

4.8.4 App

Een andere methode om gebruikers een melding te laten doen is via een smartphone applicatie. Deze applicatie zorgt er voor dat op een veilige manier verbinding gemaakt kan worden met het meldpunt, zonder dat er op de telefoon informatie achter blijft. Zie bijvoorbeeld de WebSubmit Mobile applicatie in paragraaf 4.7 als voorbeeld.

Het is mogelijk de applicatie zo in te richten dat zowel interactieve communicatie als eenweg communicatie met al dan niet gestructureerde formulieren mogelijk zijn. Omdat de applicatie vertrouwd is, is het zelfs mogelijk om meerweg-communicatie met actieve terugkoppeling mogelijk te maken.

Voordelen:

- Er is veel controle over de omgeving waarbinnen de applicatie draait en welke informatie naar buiten prijsgegeven wordt. Dit voorkomt veel van de problemen die optreden met eerder genoemde oplossingen. In het bijzonder zou Tor geïntegreerd kunnen worden in de applicatie waardoor de communicatie niet langer observeerbaar is.
- Het is een bekend concept voor gebruikers en zorgt daarmee voor veel gebruiksgemak.
- In het geval van meermalige meldingen kan er een koppeling opgezet worden met het apparaat van de gebruiker om zo terugkoppeling of meermalige melding mogelijk te maken zonder dat de melder een speciale code hoeft te onthouden.

Nadelen:

- Het vereist altijd een apparaat dat in bezit is van de gebruiker.
- Het vereist een smartphone en veroorzaakt veel ontwikkelwerk omdat voor meerdere platformen een veilige applicatie ontwikkeld moet worden.
- De aanwezigheid van de applicatie verraad het gebruik ervan. Het is lastig achteraf de applicatie

Tabel 4.1: *Samenvatting van de mogelijke communicatievormen gegeven een oplossing. Alle oplossingen zijn meervoudig te maken. De kolom terugkoppeling geeft aan of het mogelijk is voor het meldpunt om contact op te nemen met de melder.*

	Interactief	Terug-koppeling
Website		
formulier	nee, gestructureerd	geen
chatten	ja	geen
berichtenbox	ja	passief
E-Mail	nee, ongestructureerd	actief
Chatten	ja	actief
App	ja	actief

grondig te verwijderen zodanig dat er geen sporen achterblijven. Dit kan opgelost worden door deze applicatie onderdeel te maken van een andere applicatie waarvan de installatie algemeen geaccepteerd is, zoals bijvoorbeeld de Amber Alert app.
- Als (actieve) terugkoppeling wordt gebruikt is dit een risico voor de gebruiker, zijn apparaat zou dan later aan de melding gekoppeld kunnen worden.

4.9 Toetsing

In deze paragraaf zullen we de hiervoor besproken technische oplossingen, de communicatie vormen en de gegeven criteria met elkaar vergelijken.

4.9.1 Communicatievorm versus criterium

We beginnen met een aantal algemene observaties over de invloed die de verschillende communicatievormen hebben op de criteria.

- Meermalige oplossingen, en dan met name die met een terugkoppelmogelijkheid, leveren extra grote risico's op ten aanzien van de anonimiteit van de gebruiker, zijn technisch complexer om uit te voeren en lastiger voor de gebruiker (immers de koppeling moet aan de kant van de gebruiker gemaakt worden).
- Oplossingen met actieve terugkoppeling zijn bijzonder risicovol omdat er een directe koppeling naar de melder voor handen is.
- Bij de keuze tussen interactieve oplossingen en meermalige oplossingen wordt dan ook de voorkeur gegeven aan de eerste.
- De verwachte kwaliteit van een melding is hoger bij een interactieve oplossing (of een meermalige oplossing met terugkoppeling).
- Eenmalige, niet-interactieve communicatievormen zijn technisch eenvoudiger in te richten, hoewel er wel zorgvuldig met de ingestuurde data omgegaan moet worden.

4.9.2 Oplossingsrichting versus communicatievorm

In tabel 4.1 geven we een samenvatting van welke communicatievormen mogelijk zijn met welke geschetste technische oplossing. In het algemeen geldt dat iedere oplossing, zelfs een webformulier, uitgebreid kan worden tot een meermalige oplossing (bijv. doordat de melder extra informatie aan een melding toevoegt). Daarom geven we in tabel 4.1 alleen weer of de oplossing interactief of niet-interactief is en welke vorm van terugkoppeling mogelijk is. Dit wil overigens niet zeggen dat het gebruiken van een meermalige oplossing met terugkoppeling veilig of aan te raden is.

4.9.3 Oplossingsrichting versus criterium

Tabel 4.2 toetst de geschetste oplossingsrichtingen aan de gegeven criteria. We geven per criterium aan hoe tot deze scoring gekomen is:

Onobserveerbaarheid Tenzij Tor gebruikt wordt is communicatie altijd observeerbaar, zie paragraaf 4.6.1. Daaruit volgt een negatieve beoordeling voor alle oplossingen, behalve voor de app, waar Tor direct in de applicatie geïntegreerd kan worden. Als Tor wel gebruikt wordt is de onobserveerbaarheid ook goed voor alle web oplossingen. Bij de e-mail en chat-oplossingen helpt Tor niet, en blijft de onobserveerbaarheid slecht.

Confidentialiteit Bij alle oplossingen behalve chatten en e-mail garandeert een versleutelde verbinding confidentialiteit. Bij chatten en e-mail is dat in theorie ook mogelijk, maar de verwachting is dat veel melders dit niet goed kunnen toepassen.

Anonimiteit in de eindpunten Bij chatten en e-mail kan de gebruiker eenvoudig een fout maken bij het gebruik—waardoor bijvoorbeeld verzonden berichten of logs achterblijven. Ook is het lastig om metadata van mail- en chatservers te verwijderen. Daarnaast moet bij chatten een externe partij vertrouwd worden. Voor webgebaseerde oplossingen geldt dat de anonimiteit in de eindpunten over het algemeen redelijk gewaarborgd kan worden.

[18] Dit geldt alleen als het installeren van de app op zichzelf niet verdacht meer is, bijvoorbeeld omdat de applicatie is ingebed in een niet-verdachte applicatie.

Tabel 4.2: *Scoring van oplossingsrichtingen versus criteria. Mogelijke waarderingen: −, +/− en +. Hierbij betekent een + dat een oplossing beter is, dat wil zeggen, een hoge anonimiteit biedt, technisch eenvoudig is, een hoog gebruiksgemak kent, of een kwalitatief goede meldingen op zal leveren.*

	Anonimiteit m.b.t. de verbinding					
	Onobser-veerbaarheid	Confiden-tialiteit	Anonimiteit in de eindpunten	Technische eenvoud	Gebruiksgemak gebruiker	Kwaliteit melding
Website						
formulier	−	+	+/−	+/−	+/−	+/−
chatten	−	+	+/−	−	+	+
berichtenbox	−	+	+/−	−	+/−	−
E-Mail	−	−	−	+/−	−	−
Chatten	−	−	−	+/−	−	+
App	+	+	+/−[18]	−	+	+

De grootste risico's zijn onoplettende gebruikers (waardoor confidentialiteit in het geding kan komen) en een ingewikkelde oplossing aan de kant van het meldpunt. Bij een app is risico van misbruik door de gebruiker beter te minimaliseren.

Technische eenvoud Deze vloeit direct voort uit de bij de oplossingen gegeven voor- en nadelen.

Gebruiksgemak gebruiker Hoewel e-mail en chat op zich makkelijk te gebruiken zijn is het veilig gebruik ervan dat niet. In het bijzonder vallen de metadata van e-mailverkeer onder de dataretentiewet, zie ook paragraaf 5.3.1. Dit verklaart de lage score voor deze twee. In het algemeen zijn de app en de website makkelijk te gebruiken, we verwachten dat de gebruiker een voorkeur zal geven aan de interactieve oplossingen die geboden worden door de webchat en de app.

Kwaliteit melding In het algemeen verwachten we dat de kwaliteit van een melding hoog zal zijn bij interactieve oplossingen: webchatten, chatten en app. Verder verwachten we dat de meermalige niet-interactieve oplossingen e-mail en berichtenbox niet voldoende mogelijkheden bieden om kwalitatieve informatie uit te vragen. De uitzondering hierop is een webformulier dat gericht ingezet kan worden voor bepaalde meldingen (denk aan hennepplantages), waar de vraagstelling van te voren al bekend is.

Hoofdstuk 5

Juridische aspecten

In dit hoofdstuk worden de voor- en nadelen van anoniem melden via het Internet belicht vanuit juridisch perspectief. Hierbij ligt de nadruk op de positiefrechtelijke aspecten, dat wil zeggen welke rechtsregels relevant zijn. De meer abstracte normatieve aspecten, die ook een juridische component hebben, zijn al eerder aan bod geweest (in hoofdstuk 3. Het hoofdstuk beoogt een overzicht op hoofdlijnen te geven van relevante juridische aspecten, waarbij we vooral ingaan op onderdelen waarbij mogelijk verschillen bestaan tussen het bestaande telefonische meldpunt en een eventueel op te zetten Internet-meldpunt.

5.1 Verwerking van persoonsgegevens

Misdaadmeldingen zullen meestal persoonsgegevens bevatten, hetzij van een slachtoffer hetzij (wat bij anonieme meldingen vaak het geval kan zijn) van een vermoedelijke of vermeende dader. (Persoonsgegevens van de melder worden, als de anonimiteit van het systeem goed werkt, niet verwerkt.) Het meldpunt is, als de instantie die het doel en de middelen van de verwerking van de meldingen bepaalt, de verantwoordelijke voor de verwerking van deze persoonsgegevens en moet dus voldoen aan de verplichtingen van de Wet bescherming persoonsgegevens (Wbp).[1] Het CBP heeft de verwerking van persoonsgegevens in anonieme meldingen bij Stichting Meld Misdaad Anoniem als rechtmatig beoordeeld, omdat er sprake is van een legitieme grondslag (een belang dat zwaarder weegt dan het privacybelang van betrokkenen, art. 8 onder f Wbp), betrokkenen vanwege de aard van het meldpunt niet geïnformeerd kunnen worden, en inzage- en correctierechten nauwelijks van belang zijn aangezien de gegevens te kort door het meldpunt worden verwerkt [8]. Aannemend dat een Internetmeldpunt dezelfde zorgvuldigheidsnormen betracht als Stichting M., en dat de meldingen niet langer dan een paar dagen bij het meldpunt blijven opgeslagen, zal de verwerking van persoonsgegevens door het meldpunt even rechtmatig zijn als bij een telefonisch meldpunt.

Een kanttekening daarbij is dat wanneer zou blijken dat het Internetmeldpunt veel meer meldingen krijgt dan het telefonische meldpunt, en/of als de gemiddelde kwaliteit van de meldingen veel lager is, de belangenafweging anders kan uitvallen: de verwerking van persoonsgegevens zou dan relatief ernstiger zijn voor betrokkenen (onterechte beschuldigingen) terwijl het publiek belang van de melding relatief kleiner zou zijn (minder wezenlijke bijdrage aan de opsporing). Dat heeft gevolgen voor de legitieme grondslag. Bij te veel meldingen en/of te lage gemiddelde kwaliteit, biedt artikel 8 onder f Wbp geen grondslag meer en is een andere grondslag nodig. Dat betekent hetzij een wettelijke basis voor het meldpunt waarbij expliciet de beheerder van het meldpunt wordt aangewezen (grondslag artikel 8 onder c Wbp) hetzij het meldpunt onderbrengen bij een bestuursorgaan (artikel 8 onder e Wbp).

5.2 Context van anonimiteit in het strafrecht

In dit rapport gaan we niet uitgebreid in op de discussie over de rol van anonieme verklaringen in het strafrecht, maar beperken we ons tot het wijzen op de globale context hiervan. Anonieme verklaringen in het strafrecht staan op gespannen voet met het recht op een eerlijk proces. De verdediging moet bewijs kunnen

[1] Wanneer de meldingen later worden doorgegeven aan de politie, worden de gegevens politiegegevens en moet de verwerking voldoen aan de Wet politiegegevens. Er is overigens discussie mogelijk of de meldingen aan een anoniem misdaadmeldpunt niet van begin af aan al politiegegevens zijn, nu de definitie daarvan luidt 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt' (art. 1 onder a Wet politiegegevens). Ook al wordt een meldpunt door een private instantie beheerd, kan een misdaadmeldpunt mogelijk worden gezien als een onderdeel van de politietaak. Wij gaan niet verder op deze discussie in, omdat het College Bescherming Persoonsgegevens (CBP) bij Stichting M. ervan uit is gegaan dat het telefonische misdaadmeldpunt onder de Wbp valt, en een Internetmeldpunt in dit opzicht gelijk behandeld zou moeten worden als een telefonisch meldpunt.

aanvechten, en daarvoor is het belangrijk om een getuige te kunnen ondervragen tijdens de terechtzitting over zijn verklaring. Dergelijke ondervraging is lastig als de getuige anoniem is. In de jaren '80 en '90 was er veel discussie over dit spanningsveld.[2] Inmiddels zijn de contouren van het gebruik van anoniem getuigenbewijs wel uitgekristalliseerd, passend in een internationale tendens dat het gebruik van anoniem getuigenbewijs steeds verder wordt genormaliseerd [22].

Het Wetboek van Strafvordering erkent drie vormen van min of meer anoniem bewijs: de verklaring van een bedreigde getuige afgelegd bij de rechter-commissaris, de verklaring van een beperkt anonieme getuige en de schriftelijke verklaring van een anoniem gebleven getuige [11, p. 4]. Bij de eerste twee vormen is de identiteit van de getuige niet bekend bij de verdachte maar is de getuige wel bekend bij justitie zodat deze ondervraagd kan worden via de rechter-commissaris of de zittingsrechter. Voor de context van dit rapport is de derde vorm het meest relevant: 'een schriftelijk bescheid houdende de verklaring van een persoon wiens identiteit niet blijkt' (art. 344a lid 3 Sv), oftewel de verklaring die een anonieme getuige bij de politie of elders heeft afgelegd; een dergelijke verklaring kan alleen voor het bewijs worden gebruikt als er 'in belangrijke mate steun' is in andersoortig bewijsmateriaal en als de verdediging niet te kennen geeft de persoon te willen (doen) ondervragen (art. 344a lid 3 Sv). De rechter zal de betrouwbaarheid van de verklaring, die dus alleen als steunbewijs kan dienen, moeten motiveren in het vonnis [11, p. 6]. In de praktijk blijkt de verklaring van (bedreigde) anonieme getuigen over het algemeen weinig bruikbare informatie te bevatten voor het bewijs [11, p. 4]. Als bewijsmateriaal heeft een anonieme verklaring daarom maar beperkt nut, maar een anonieme verklaring kan wel waardevol zijn als sturingsinformatie voor het opsporingsonderzoek [11, p. 6 en 8].

Ondanks de beperkingen van (beperkt) anonieme verklaringen als bewijs, stimuleert het beleid sinds enkele jaren wel het doen van (beperkt) anonieme aangifte. Binnen het programma Veilige Publieke Taak (VPT) zijn ter verhoging van de aangiftebereidheid informatiebladen ontwikkeld voor werkgevers, werknemers en getuigen/slachtoffers, waarin mogelijkheden van (deels) anonieme aangifte worden uitgelegd.[3] Zo kan een werknemer aangifte doen op naam met domiciliekeuze (waarbij wel de naam wordt geregistreerd maar een ander correspondentieadres wordt opgenomen, zodat het woonadres onbekend blijft) of aangifte doen onder nummer, waarbij een uniek nummer wordt toegekend en de identiteit en het feitelijke adres van de werknemer alleen bekend zijn bij het Slachtofferloket van de politie. De werknemer kan dan wel, zo nodig, worden verhoord of opgeroepen om bij de rechter de aangifte toe te lichten, maar de identiteit kan dan worden afgeschermd (via videoconferentie, vermomming of stemvervorming, als de rechter dat toestaat), zodat verdachte en diens advocaat de identiteit niet leren kennen [23]. Voor getuigen van agressie in de zorgsector die deze vormen van (gedeeltelijke) anonimiteit niet voldoende vinden en die echt anoniem willen blijven, verwijst het beleid naar Stichting M.: 'Deze landelijke meldlijn is niet van de politie, maar van een onafhankelijke stichting. Er werkt een klein team van zeer goed opgeleide mensen met maar één doel voor ogen: uw anonimiteit beschermen. M. biedt een vangnet voor als u wel wilt melden, maar niet bekend wilt worden' [32]. Dit geeft tegelijkertijd aan dat de bestaande vormen om anonimiteit bij aangifte in het strafproces te faciliteren, uitgaan van gedeeltelijke en ophefbare anonimiteit en niet, zoals bij het meldpunt in onderhavige studie, van zo sterk mogelijke anonimiteit. Het nut van anoniem (Internet)melden moet dan ook alleen worden gezocht in het verkrijgen van start- of sturingsinformatie voor de opsporing en niet (ook) in de eventuele bewijswaarde van meldingen. Een aandachtspunt in dat licht is, zoals uit de voor dit onderzoek gehouden expertworkshop naar voren kwam, dat burgers die misdaad anoniem melden vaak denken dat ze een belangrijke bijdrage aan het 'oplossen' van de misdaad leveren en zich meestal niet realiseren dat hun melding niet bruikbaar is als bewijs; verwachtingsmanagement bij potentiële melders is daarom een belangrijk aandachtspunt bij de profilering van het meldpunt.

5.3 Juridische mogelijkheden om identiteit van melders te achterhalen

Voor zover anonimiteit technisch niet absoluut kan worden afgedwongen en er dus een zekere mogelijkheid bestaat om de identiteit van een melder te achterhalen, is het relevant te kijken welke juridische mogelijkheden er zijn om de anonimiteit van een melder te doorbreken. We maken daarbij onderscheid tussen politie/justitie, andere overheidsdiensten en private partijen.

5.3.1 Politie en justitie

Het meest relevant is de vraag onder welke omstandigheden politie of justitie de identiteit van een anonieme melder zou kunnen achterhalen. Vier typen bevoegd-

[2] Zie EHRM 20 november 1989, Kostovski t. Nederland, App.nr. 11454/85 (dat de Nederlandse praktijk van anonieme getuigenverklaringen als onrechtmatig beoordeelde), de daaropvolgende Wet getuigenbescherming, Stb. 1993, 603 en de kritiek op de op die wet gebaseerde uitspraken van Garé [12].

[3] *Kamerstukken II* 2011/12, 28 684, nr. 344, p. 6.

heden zijn daarvoor van belang. Ten eerste het onderscheppen van communicatie. We nemen aan dat de politie het meldpunt zelf niet zal willen afluisteren (en dat de rechter-commissaris daar in elk geval geen toestemming voor zal geven), maar het is mogelijk dat er een tap loopt op iemand die een melding doet. Bij het telefonisch meldpunt is de afspraak gemaakt dat er een technische voorziening wordt getroffen om te voorkomen dat in zo'n situatie het gesprek met het meldpunt wordt opgenomen: via nummerherkenning wordt het 0800-nummer van het meldpunt herkend en dan wordt het gesprek automatisch uitgefilterd [29]; dit is vergelijkbaar met de technische regeling die bij advocaten is getroffen (zie Bongers et al. [4]).

Een dergelijke oplossing om het tappen van een melding te voorkomen is relatief eenvoudig bij een telefoontap, maar mogelijk ingewikkelder bij Internet. Een Internettap kan bestaan uit een e-mailtap (waarbij alle ingaande en/of uitgaande e-mail van een bepaald IP-adres of e-mailadres wordt getapt) of een IP-tap (waarbij al het IP-verkeer wordt getapt en vervolgens uitgefilterd). Om het automatisch herkennen en filteren van een bericht aan het meldpunt te faciliteren, moet het meldpunt daarom in elk geval een vast e-mailadres of IP-adres gebruiken. Of een dergelijke filtering bij een Internettap zo kan worden geconfigureerd dat de integriteit van de Internettap als geheel niet wordt gecompromitteerd, kan binnen het bestek van deze quickscan niet worden onderzocht; dat is een aandachtspunt voor nader onderzoek. Indien een filtering op basis van nummerherkenning niet mogelijk is, kan filtering wel plaatsvinden in de fase van analyse en selectie van het IP-verkeer, maar daarbij bestaat het risico dat de melding wordt gelezen. In dat geval zijn organisatorische maatregelen nodig die voorkomen dat de politie kennis neemt van de inhoud van de melding, waarbij selectie en filtering van IP-verkeer door een andere instantie dan de politie plaatsvindt, maar dat past niet goed binnen de huidige opzet van IP-taps. Hoewel het risico dat er een IP-tap loopt bij iemand die een anonieme melding doet klein is, moet dit punt wel afgedicht worden, bij voorkeur via een technische oplossing van automatische filtering via nummerherkenning van het IP- of e-mailadres.

Het tweede type bevoegdheid is het vorderen van gegevens. Vooral belangrijk is het vorderen van verkeersgegevens (art. 126n/u/zh Sv). Bij het telefonisch meldpunt is een regeling getroffen waarbij de politie in zeer uitzonderlijke gevallen verkeersgegevens kan opvragen, bijv. wie er met het meldpunt heeft gebeld. Volgens artikel 5.1 van de Aanwijzing opsporingsbevoegdheden[4] is hiervoor toestemming nodig van het College van Procureurs-Generaal (CPG) na advies van de Centrale Toetsingscommissie; volgens de Instructie Meld Misdaad Anoniem van het CPG mogen verkeersgegevens betreffende het meldpunt alleen worden opgevraagd in situaties van onmiddellijk dreigend levensgevaar, waarbij de gegevens alleen mogen gevorderd als de inlichtingen nodig zijn om het desbetreffende leven te redden [9][3, p. 35]. Volgens Boes [3, p. 36] is tussen 2005 en 2009 vijf maal een verzoek ingediend om verkeersgegevens over het meldpunt te mogen vorderen en is in geen van deze gevallen het verzoek gehonoreerd.

In plaats van verkeersgegevens te vorderen betreffende het meldpunt, kan het ook voorkomen dat een contact met het meldpunt voorkomt bij verkeersgegevens die over een persoon worden gevorderd, als die persoon in de voorkomende periode met het meldpunt heeft gebeld. Ook op die situaties is de Instructie Meld Misdaad Anoniem van toepassing en moet de procedure van CTC-advies en toestemming van het College van Procureurs-Generaal worden gevolgd. De Instructie stelt: 'Ook indien in een lopend opsporingsonderzoek aan de hand van verkeersgegevens of een tap blijkt dat een persoon met M. heeft gebeld, dient deze instructie te worden gevolgd' [9, p. 2]. Het is niet helemaal duidelijk wat dit betekent: het gaat dan immers niet meer om toestemming om het verkeersgegeven te mogen vorderen en daarmee de identiteit van een melder te achterhalen; in dit geval heeft de politie het gegeven al. Vermoedelijk betekent het dat de politie het verkeersgegeven alleen mag gebruiken nadat de benodigde toestemming is verkregen, in een acuut levensbedreigende situatie. Praktisch betekent dit dat wanneer het telefoonnummer van het meldpunt in een lijst met gevorderde gegevens voorkomt, dit verwijderd zou moeten worden, om te voorkomen dat het gegeven in een politiebestand terecht komt en onverhoopt alsnog ergens voor wordt gebruikt. De Instructie meldt echter niets over vernietiging als er geen toestemming wordt gevraagd of verkregen. Ons is niet bekend hoe in de praktijk met deze situatie wordt omgegaan.

Voor een meldpunt via Internet kan dezelfde lijn worden gevolgd als bij het telefonisch meldpunt; de Aanwijzing opsporingsbevoegdheden en de Instructie Meld Misdaad Anoniem zouden simpelweg uitgebreid kunnen worden met een verwijzing naar het Internetmeldpunt. Er zijn wel twee relevante verschillen tussen Internet en telefonie. Ten eerste bepaalt de Wet bewaarplicht telecommunicatiegegevens[5] dat verkeersgegevens betreffende vaste en mobiele telefonie gedurende één jaar moeten worden bewaard door de telecomaanbieder, terwijl verkeersgegevens betreffende Internet (Internettoegang, e-mail, Internettelefonie) zes maanden moeten worden bewaard. Vooral van belang is dat alleen bij e-mail de contactadressen (wie mailt met wie) bewaard worden; bij andere vormen van In-

[4] *Staatscourant 2011*, 3240.

[5] *Stb.* 2009, 333, aangepast bij wet van 6 juli 2011, *Stb.* 2011, 350.

ternetverkeer (zoals chat of webformulieren) valt het adres niet onder de bewaarplicht. Om de situatie te voorkomen dat via een vordering verkeersgegevens betreffende een persoon naar voren zou komen dat deze persoon (of preciezer: diens aansluiting) contact heeft gehad met het meldpunt, kan dus beter een configuratie via web, webchat, instant messaging of een app worden gekozen dan een configuratie via e-mail. Daarbij moet wel weer worden aangetekend dat verkeersgegevens betreffende web-, chat- of appgebruik wel bewaard kunnen worden door de aanbieder op basis van diens bedrijfsbelang, ook al vallen ze niet onder de bewaarplicht, en dat het theoretisch mogelijk is dat een aanbieder dergelijke gegevens langer dan zes maanden bewaart als het bedrijfsbelang dat rechtvaardigt. Dat zal in de praktijk vermoedelijk nauwelijks het geval zijn.

Ten tweede is relevant dat het onderscheid tussen verkeersgegevens en inhoud van communicatie moeilijker te maken is bij Internet dan bij telefonie. Zoals een recente analyse van dit onderscheid van Koops en Smits [18] aantoont, is het weliswaar bij bepaalde toepassingen nog steeds mogelijk om de verkeersgegevens technisch te onderscheiden van de inhoud, maar wordt die scheiding allengs moeilijker naarmate er een grotere variëteit aan snel veranderende Internetprotocollen komt. Bovendien geven verkeersgegevens, zeker in een Internetomgeving, steeds meer zicht op de (soms letterlijke en soms globale) inhoud van communicatie. Koops en Smits [18, p. 146] concluderen dan ook dat verkeersgegevens behorende bij Internet (met uitzondering van e-mail) integraal onder het juridische beschermingsregime van inhoud van communicatie zouden moeten vallen, omdat ze er onlosmakelijk mee verknoopt of anderszins even gevoelig van aard zijn. Nu is dit punt minder van belang, zolang de Instructie maar van toepassing is op alle gevallen waarin verkeersgegevens worden gevorderd, en ook wordt nageleefd in gevallen waarin bij verkeersgegevens die over een persoon worden gevorderd contactgegevens met het meldpunt omvatten.

Naast verkeersgegevens kunnen ook andere gegevens worden gevorderd waaruit de identiteit van een melder zou kunnen blijken (art. 126nc/uc/zk en volgende Sv). Daarvan zijn geen voorbeelden uit de praktijk bekend. Het telefonisch meldpunt vernietigt aantekeningen van gesprekken direct na het gesprek [3, p. 34], wat vermoedelijk betekent direct nadat de aantekeningen verwerkt zijn in een melding die wordt doorgegeven dan wel zodra besloten wordt de melding niet door te zetten. In de korte tijd dat de aantekeningen van gesprekken wel voorhanden zijn, kan de politie deze in theorie vorderen; naar de geest van de wet zou daarop ook de Instructie van toepassing moeten zijn, hoewel de letter niet over deze vorm van gegevensgaring spreekt (vgl. [3, p. 36]).

Hetzelfde geldt voor het derde type bevoegdheid: doorzoeking en inbeslagneming. De Instructie heeft geen betrekking op doorzoeking van het Meldpunt, maar we mogen aannemen dat die er wel op van toepassing zou moeten zijn, en dat geldt evengoed voor een eventueel op te zetten Internetmeldpunt waarop de aangepaste Instructie van toepassing zou worden. Dat de Instructie ook op dit soort situaties van toepassing wordt, is belangrijk voor een Internetmeldpunt, aangezien daarbij, anders dan bij het telefonische meldpunt, meer sporen achterblijven. Het vernietigen van sporen van chats of webmeldingen is ingewikkelder dan het vernietigen van aantekeningen in een papierversnipperaar. Met forensische software kunnen sporen van uitgewiste gegevens op harde schijven worden achterhaald; om deze mogelijkheid uit te sluiten zouden meldpuntmedewerkers voor de vernietiging van chats, webmeldingen en aantekeningen ook gespecialiseerde software moeten gebruiken. Aangezien het wissen van sporen technisch een uitdaging is (zie par. 4.6.6), bestaat er enig risico dat de politie, indien zij per se de identiteit van een melder zouden willen achterhalen, doorzoeking doet bij het meldpunt en computers in beslag neemt om forensisch onderzoek te doen. Dit onderstreept het belang van het van toepassing maken van de Instructie op alle opsporingshandelingen, inclusief vorderen van gegevens en doorzoeking.

Belangrijk is verder dat in het kader van een doorzoeking of inbeslagneming elders dan bij het Meldpunt zelf ook informatie boven water kan komen over een melding. Zo kan bij een doorzoeking de computer onderzocht worden van iemand die contact heeft gehad met het meldpunt, waarbij—afhankelijk van de configuratie—sporen van dat contact in de computer achtergebleven zijn (denk aan tijdelijke Internetbestanden of verwijderde chatlogs die met forensische programmatuur te traceren zijn). Wat ons betreft is deze situatie vergelijkbaar met de situatie waarin de politie via verkeersgegevens erachter komt dat iemand contact met het meldpunt heeft gehad—een situatie waarop als boven geconstateerd de Instructie van toepassing is (hoewel onduidelijk is wat dit in de praktijk betekent). De Instructie zou in dat licht generiek van toepassing moeten zijn niet alleen op een eventueel op te zetten Internetmeldpunt naast het telefonische meldpunt, maar ook op alle handelingen waarbij de politie gegevens verkrijgt over contact met het meldpunt, ongeacht de precieze bevoegdheid die is uitgeoefend. Het maakt voor de anonimiteitsopheffing immers niet uit of deze via een tap, gegevensvordering, doorzoeking of anderszins plaatsvindt; in alle gevallen is er bij anonimiteitsopheffing immers een afbreukrisico van het anonieme meldpunt als hulpmiddel in de opsporing (vgl. [9]).

Het vierde type ten slotte is het oproepen van getuigen: theoretisch is denkbaar dat de politie een medewerker van het meldpunt oproept om te getuigen in een straf-

zaak, waarbij de medewerker verplicht zou zijn om te antwoorden op vragen rond de identiteit van een melder. (De medewerker heeft immers geen beroepshalve verschoningsrecht, noch een verschoningsrecht op basis van zelfbelasting van zichzelf of een naaste.) Zoals Boes [3, p. 36] aangeeft, is het echter onmogelijk bij het meldpunt M. te achterhalen wie precies welke melding heeft opgenomen (tenzij dit wellicht binnen een of twee etmalen na de melding bij een opvallende zaak gebeurt, maar bij getuigenoproepen zal er veel meer tijd zitten tussen de melding en de getuigenverklaring). Ook hiervoor geldt onzes inziens dat de Instructie van toepassing zou moeten zijn, ook in het geval van een Internetmeldpunt.

In aanvulling op deze bespreking van bevoegdheden moet nog worden opgemerkt dat, waar de Instructie op papier een heldere keuze maakt om anonimiteit alleen in uitzonderlijke, levensbedreigende situaties te kunnen opheffen, er aanwijzingen zijn dat de politie in de praktijk toch regelmatig druk uitoefent op medewerkers van het meldpunt om achter de identiteit van een melder te komen, een enkele keer zelfs door te dreigen met gijzeling. Hoewel dergelijke druk van de politie in de voor dit onderzoek gehouden expertworkshop een 'gezonde spanning' werd genoemd, bestaat er een aanzienlijk risico voor de anonimiteit als de medewerkers van het meldpunt niet stevig genoeg in hun schoenen staan. Dit is van belang indien bij een Internetmeldpunt aanzienlijk meer meldingen zouden binnenkomen die door aanzienlijk meer medewerkers zouden worden behandeld; de medewerkers zouden op dit punt goed geïnformeerd en getraind moeten worden. Minstens zo belangrijk lijkt ons training van politiemedewerkers om de geest van de Instructie Meld Misdaad Anoniem ook tussen de oren van de politie op de werkvloer te krijgen.

Op basis van de bespreking van opsporingsbevoegdheden kunnen we constateren dat er weinig relevante verschillen zijn, in juridisch opzicht, tussen een telefonisch en een Internetmeldpunt. Onderzocht zou moeten worden of bij een Internettap automatisch de communicatie met een Internetmeldpunt afdoende weggefilterd kan worden, zoals dat bij de telefoontap momenteel wordt beoogd. Vanuit het oogpunt van dataretentie heeft een Internetmeldpunt, in het bijzonder de configuraties die niet via e-mail werken, zelfs de voorkeur boven een telefonisch meldpunt, omdat er minder sporen van het contact tussen melder en meldpunt (verplicht) worden opgeslagen, die via een vordering aan de communicatieaanbieder over het communicatieverkeer van de gebruiker bij de politie terecht zouden kunnen komen. Die situatie valt weliswaar onder de Instructie, zodat de gegevens alleen in levensbedreigende situatie ter levensredding mogen worden gebruikt, maar ons is niet bekend of in de praktijk gegevens worden vernietigd als het niet levensbedreigende situaties betreft.

5.3.2 Overige overheidsinstanties

Hoewel de politie het meeste belang lijkt te hebben om in incidentele gevallen de identiteit van een melder te achterhalen, kunnen ook andere overheidsdiensten een dergelijk belang hebben—denk aan de AIVD, de Belastingdienst, de gemeente of sociale zekerheidsdiensten. In het kader van deze quickscan is het niet mogelijk om de bevoegdheden van al deze diensten in kaart te brengen. Wat we wel kunnen zeggen is dat de bevoegdheden van de AIVD als vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 zeer ruim zijn, en dat deze dienst bijvoorbeeld via aftappen (art. 25 Wiv 2002), hacken (art. 24 Wiv 2002) of het opvragen van verkeersgegevens (art. 28 Wiv 2002) informatie kan verkrijgen over wie een melding gedaan heeft. Voor zover ons bekend bestaat er voor inlichtingen- en veiligheidsdiensten (ivd's) geen soortgelijke instructie als die voor politie en justitie geldt, die aangeeft dat alleen in acuut levensbedreigende situaties anonimiteit mag worden opgeheven. Deze diensten zouden dus, in juridisch opzicht, alle tot hun beschikking staande bevoegdheden kunnen gebruiken om in voorkomende gevallen de identiteit van een melder te achterhalen. Het is niet bekend in welke praktijksituaties de diensten daar daadwerkelijk belang bij zouden hebben en van hun bevoegdheden gebruik zouden maken. Hoewel wij niet verwachten dat de wetenschap dat ivd's anonimiteit zouden kunnen doorbreken in het algemeen een verkillend effect zou hebben op de bereidheid van burgers om misdaad te melden, gaat het niet om een puur theoretisch risico voor anonimiteitsdoorbreking: denkbaar is bijvoorbeeld dat een jongere die zijn vriendengroep langzaam ziet radicaliseren en plannen hoort van sommigen om naar Syrië te reizen, geen melding zal doen bij een anoniem meldpunt, uit vrees voor sociale uitstoting of ergere represailles indien zijn identiteit via de AIVD onverhoopt achterhaald en bekend zou worden. Aangezien gegevens ontbreken over situaties waarin ivd's anonimiteit van melders (zouden willen) doorbreken, is het moeilijk om het risico van anonimiteitsdoorbreking, en een mogelijk verkillend effect op melders, in dit opzicht in te schatten.

Voor andere overheidsdiensten geldt dat deze weliswaar als bestuursorganen aanzienlijke bevoegdheden hebben om inlichtingen of bescheiden te vorderen, maar geen aftapbevoegdheden hebben en ook geen specifieke bevoegdheid om verkeersgegevens te vorderen. Het risico van anonimiteitsdoorbreking door andere overheidsdiensten is navenant kleiner dan bij ivd's en lijkt ons geen rol te spelen in de afweging over een Internetmeldpunt.

5.3.3 Private partijen

Private partijen mogen geen communicatie aftappen (wat strafbaar is onder art. 139c Wetboek van Strafrecht). Wel mag een telecomaanbieder (van de melder of het meldpunt) rechtmatig de inhoud van communicatie inzien als dat noodzakelijk is voor technische controle van de dienstverlening, maar het risico dat daardoor de communicatie tussen melder en meldpunt wordt afgetapt is verwaarloosbaar.

Private partijen mogen wel verzoeken om inzage in gegevens. Denkbaar is dat een private partij die betrokken is bij de zaak waaromtrent een anonieme melding is gedaan, de identiteit van de melder zou willen achterhalen. Zij zouden dan bij de telecomaanbieder van het meldpunt verkeersgegevens kunnen opvragen. Telecomaanbieders maken dan een belangenafweging tussen het belang van de verzoeker om gegevens in te zien en het belang van de betrokkene (de melder) om de gegevens afgeschermd te houden. In de enigszins vergelijkbare situatie waarin een benadeelde een Internethostingaanbieder vraagt om NAW-gegevens of andere beschikbare identificerende gegevens te leveren van degene die hem (naar zijn mening) heeft benadeeld (bijvoorbeeld door een smadelijke uiting), moet de aanbieder adresgegevens verstrekken als de inhoud aannemelijkerwijs onrechtmatig is, de verzoeker een belang heeft bij de identificerende gegevens en deze niet op een andere manier kunnen worden achterhaald, en de belangenafweging in het voordeel van de verzoeker uitvalt.[6] Nu zal in het geval van een anoniem Internetmeldpunt de belangenafweging vrijwel altijd in het voordeel van de anonieme melder uitvallen. Nu er een normatief kader ligt waarbij de politie alleen in acuut levensbedreigende situaties identificerende gegevens van een melder mag opvragen, zodat in de publiekrechtelijke belangenafweging vrijwel altijd het belang van de anonieme melder prevaleert, zal in de privaatrechtelijke belangenafweging alleen in even uitzonderlijke—levensbedreigende—situaties het belang van de verzoekende partij zwaarder wegen. Dergelijke situaties zijn moeilijk voorstelbaar, zodat het juridische risico van anonimiteitsopheffing door private partijen ook als verwaarloosbaar klein kan worden gezien. Een voorwaarde daarvoor is echter wel dat de telecomaanbieder van het meldpunt, die de belangenafweging maakt, geheel doordrongen is van het normatieve kader dat geldt voor de politie en van het grote belang van anonimiteit van melders; dit zou met voorlichting, maar wellicht ook contractueel of via een gedragscode, kunnen worden bewerkstelligd.

[6] HR 25 november 2005 (Lycos/Pessers), ECLI:NL:HR:2005:AU4019.

5.4 Aansprakelijkheidsrisico's voor het meldpunt

Indien de anonimiteit van een melder onverhoopt wordt doorbroken en deze daardoor schade lijdt (bijvoorbeeld omdat zij moet verhuizen of ontslagen wordt), kan het meldpunt of de politie dan aansprakelijk worden gesteld? Dat zal afhangen van de juridische status en de reikwijdte van het meldpunt (bij een overheidsmeldpunt in het kader van de publiekrechtelijke taak van misdaadbestrijding ligt het aansprakelijkheidsrisico lager dan bij een privaat meldpunt betreffende maatschappelijke misstanden). Verder hangt het vooral af de manier waarop de identiteit bekend raakt en de mate van (on)zorgvuldigheid die in acht is genomen om de anonimiteit te waarborgen. We mogen aannemen dat het meldpunt veel moeite doet (zowel technisch als organisatorisch) om de anonimiteit van melders te waarborgen; alleen als medewerkers van het meldpunt aanmerkelijk nalatig zijn (bijvoorbeeld door aantekeningen van gesprekken bij het oud papier op straat te zetten), bestaat er een zeker aansprakelijkheidsrisico. Gezien de gevoeligheid van de anonimiteit van misdaadmelders, rust er wel een relatief grote verantwoordelijkheid op het meldpunt en haar medewerkers om zorgvuldig om te gaan met meldingen en om technische, organisatorische en mogelijk ook juridische maatregelen te treffen om het risico op het bekend raken van de identiteit van melders zo klein mogelijk te houden. Dat zal voor een Internetmeldpunt op zich niet anders zijn dan voor het telefonische meldpunt. Wel is van belang dat aansprakelijkheidsrisico's toenemen naarmate er meer meldingen worden gedaan of meldingen een ruimer scala aan gedragingen dan ernstige misdrijven zouden betreffen; mocht een Internetmeldpunt door laagdrempeligheid leiden tot een significante toename aan meldingen, dan zou het aansprakelijkheidsrisico groter kunnen worden en zouden (nog) zwaardere maatregelen nodig zijn om het risico op identiteitsdoorbreking van melders zo klein mogelijk te houden.

Wel moet erop worden gelet, afhankelijk van de gekozen configuratie, dat de gegevens die een melder aanlevert —indien deze worden overgenomen in een melding die vervolgens aan de politie of andere afnemers wordt gestuurd—geen (direct of indirect) identificerende gegevens bevat. Bij het telefonisch meldpunt zit er een natuurlijke vertaalslag tussen het verhaal van de melder en wat de medewerker opschrijft in de melding; bij een Internetmeldpunt zou de verleiding kunnen bestaan om teksten van de melder rechtstreeks te kopiëren in een melding, waarbij het risico van (ook indirect) identificerende gegevens groter is. Zoals al in technische analyse (zie par. 4.2.3) is opgemerkt, zou het systeem zodanig moeten worden ingericht dat er geen dataverkeer mogelijk is tussen de ter-

minal waarop informatie zichtbaar is en het systeem waarin de uiteindelijke melding gemaakt wordt. Verder zijn strakke procedures zoals Stichting M. die hanteert, bijvoorbeeld om elke melding door een andere medewerker te laten tegenlezen op potentieel identificerende informatie, evenzeer belangrijk voor een Internetmeldpunt.

Vanuit juridisch oogpunt valt te overwegen om de zorgvuldigheid van de omgang met meldingen te versterken door de technisch-organisatorische maatregelen ook juridisch te verankeren, bijvoorbeeld door een verwijzing in het arbeidscontract met medewerkers naar zorgvuldigheidsnormen en de te volgen procedures voor zorgvuldige omgang met meldingen, die bijvoorbeeld in een gedragscode zijn vastgelegd. Dat is niet alleen van belang voor medewerkers die meldingen opnemen, maar vooral ook voor de systeembeheerder van een Internetmeldpunt, die uit de aard van de functie meer mogelijkheden heeft om de IP-afkomst van een melding te traceren. Door verwijzing naar de gedragscode in het arbeidscontract (of anderszins een adequate bekendmaking onder werknemers) zal de open norm van het goed werknemerschap (art. 7:611 Burgerlijk Wetboek) worden ingekleurd door de verplichting zich te houden aan de gedragscode, wat kan bijdragen aan de naleving ervan op de werkvloer. Juridische (contractuele) verankering van technische of organisatorische gedragsnormen om anonimiteit te waarborgen is daarnaast noodzakelijk wanneer de verwerking of opslag van meldingen extern zou worden uitbesteed, bijvoorbeeld op een server in een datacentrum of in de cloud, waarbij externe partijen toegang hebben tot de server.

5.5 Hoeveelheid, kwaliteit en rol van meldingen vanuit juridisch perspectief

Een van de onderzoeksvragen betreft de te verwachten gevolgen van anoniem melden via Internet voor de hoeveelheid en kwaliteit van meldingen en de rol van anonieme meldingen in de opsporing. Vanuit juridisch perspectief valt weinig te zeggen over de te verwachten hoeveelheid of kwaliteit van Internetmeldingen—er zijn geen juridische normen die het voor burgers meer of minder aantrekkelijk maken om misdaad via het Internet in plaats van via de telefoon te melden. Als we aannemen, op basis van het interview en de workshop, dat een Internetmeldpunt laagdrempeliger kan zijn dan een telefonisch meldpunt en dat daardoor de hoeveelheid meldingen toeneemt (en wellicht navenant de gemiddelde kwaliteit afneemt), welke gevolgen heeft dit dan voor de rol van meldingen in de opsporing?

Zoals geconcludeerd in paragraaf 5.2 over de context van anonimiteit in het strafrecht, worden Meld Misdaad Anoniem-meldingen niet gebruikt als bewijs, maar als start- of sturingsinformatie. Anonieme meldingen mogen volgens de jurisprudentie worden gebruikt om een opsporingsonderzoek te starten (dan wel om een lopend onderzoek nader richting te geven). De vraag is vooral of op basis van een anonieme melding een redelijke verdenking (dat wil zeggen een redelijk vermoeden van schuld aan een strafbaar feit) mag worden aangenomen, wat de drempel is om bepaalde opsporingsbevoegdheden, zoals een doorzoeking, te mogen inzetten. De jurisprudentie eist meestal dat de politie enig aanvullend onderzoek doet om de informatie uit de melding te verifiëren. De eisen aan dit aanvullend onderzoek kunnen echter verschillen, afhankelijk van bijvoorbeeld de urgentie of de aard van de melding; Brinkhoff concludeert (voorzichtig) op basis van jurisprudentieonderzoek dat bijvoorbeeld bij vuurwapens de mogelijke gevaarzetting groter en de drempel voor aanvullend onderzoek lager is dan bij een melding van de aanwezigheid van drugs [5]. Het enkele feit dat een melding tot spoed noopt, is echter niet voldoende om zonder nader onderzoek een redelijke verdenking aan te nemen.[7] Brinkhoff [5] concludeert echter dat 'over het algemeen weinig eisen worden gesteld aan het nadere onderzoek. De redelijke verdenking wordt betrekkelijk snel aangenomen. Als deze lijn zich voortzet, is het denkbaar dat *de facto* een enkele melding bij de M-lijn voldoende is voor de aanname van de redelijke verdenking. Hiermee zou ons inziens in dit soort zaken sprake zijn van een uitholling van het begrip redelijke verdenking. Dat dit onwenselijk is, behoeft weinig betoog. Immers het enkele feit dat een burger bij de M-lijn een anonieme melding doet over een andere burger, wat er ook zij van de juistheid van deze informatie, rechtvaardigt in mijn ogen niet ogenblikkelijk de inzet van een dwangmiddel of de start van een strafrechtelijk onderzoek. Hier is wel degelijk aanvullend onderzoek voor nodig.'

Het is moeilijk te voorspellen wat de gevolgen zouden zijn van een eventuele toename in hoeveelheid meldingen bij oprichting van een anoniem Internetmeldpunt. Enerzijds kan het gevolg zijn dat de politie zoveel meldingen krijgt waar iets mee zou moeten gebeuren, dat er te weinig tijd en capaciteit is om nader onderzoek te doen, zodat het risico bestaat dat de tendens die Brinkhoff schetst wordt voorgezet: de enkele melding van een schijnbaar ernstig feit zou dan al voldoende zijn voor de politie om in actie te komen. Dat zou het systeem van het strafrecht, waarbij de redelijke verdenking, gebaseerd op feiten en omstandigheden, als startpunt van opsporingsonderzoek een dragende pijler is, onder druk zetten.

[7] HR 13 juli 2010, ECLI:NL:HR:2010:BM2492.

Anderzijds zou het gevolg kunnen zijn dat in de grotere hoeveelheid meldingen meer kaf tussen het koren zit, dat het meldpunt zelf niet altijd goed zal kunnen filteren, en dat de politie zich genoodzaakt voelt om scherper te selecteren en meldingen te verifiëren met aanvullend materiaal, omdat anders de waarde van anonieme meldingen te sterk zou verwateren. Ook is denkbaar dat, als de politie in meer zaken opsporing zou starten enkel gebaseerd op een anonieme melding, en zich hierbij bijvoorbeeld een aantal zaken van pertinent onrechtmatige opsporing zou voordoen, de rechter strakker zal controleren op de rol van anonieme startinformatie en een wat zwaardere invulling zou gaan geven aan het criterium van aanvullende informatie.

Hoe ook precies tussen deze twee mogelijkheden de rol van anonieme meldingen in de opsporing zich zou ontwikkelen, moeten in elk geval ook een aantal mogelijke neveneffecten een rol spelen bij de afweging al dan niet een anoniem Internetmeldpunt op te zetten. Beleidsmakers moeten zich realiseren dat, als het eerste scenario werkelijkheid zou worden van een overbelast politieapparaat dat wegens tijdgebrek meer afgaat op anonieme meldingen zonder nadere controle, het risico toeneemt op schadeclaims van burgers die slachtoffer zijn geworden van onrechtmatige opsporingshandelingen. Zo zou een burger die anoniem onterecht wordt beschuldigd van kindermisbruik, zich gedwongen kunnen voelen te verhuizen omdat hij sociaal wordt uitgestoten vanwege het opsporingsonderzoek, ook al hebben politie en justitie achteraf kenbaar gemaakt dat het onderzoek op onterechte informatie was gebaseerd. In dergelijke gevallen waarbij de politie onvoldoende moeite heeft gedaan om de anonieme melding na te trekken, is een succesvolle onrechtmatigedaadsactie tegen de overheid niet denkbeeldig. Verder betekent de verwachte laagdrempeligheid van Internetmeldingen dat het niet alleen makkelijker wordt voor burgers om misdaad te melden, maar ook om andere dingen te doen (in het verlengde van een mogelijke 'klikcultuur' waarop we in het volgende hoofdstuk nader ingaan). Zo wijst Brinkhoff (2008) erop dat de oncontroleerbaarheid van anonieme meldingen

> 'kan leiden tot misbruik van de M-lijn in die zin dat onder meer het risico bestaat dat opzettelijk valse informatie wordt doorgegeven. Denk hierbij bijvoorbeeld aan de anonieme beller die een ander om wat voor een reden dan ook een hak wil zetten en daarom bewust onware informatie doorgeeft. In het geval deze valse melding op de vindplaats van (vuur)wapens ziet, zal de politie zonder veel nader onderzoek snel tot actie willen overgaan. Denk bij het gevaar voor misbruik ook aan criminelen die uit concurrentieoverwegingen (valse) informatie over andere criminelen doorgeven aan de M-lijn, teneinde een ingrijpen van de politie uit te lokken. Voorts bestaat de niet geheel theoretische mogelijkheid dat de politie misbruik zal maken van de M-lijn. Te denken valt hierbij bijvoorbeeld aan het door opsporingsambtenaren van de Criminele Inlichtingen Eenheid (CIE) melden van informatie bij de M-lijn ter afscherming van een informant.'

Deze neveneffecten van potentieel misbruik van een laagdrempeliger Internetmeldpunt moeten worden onderkend en nadrukkelijk betrokken bij de beleidsafweging om al dan niet een dergelijk meldpunt op te zetten. Er valt vanuit dit perspectief het nodige voor te zeggen om een Internetmeldpunt niet (substantieel) laagdrempeliger te maken dan het telefonische meldpunt. Met name pleit het punt van mogelijk misbruik ook voor configuraties waarbij er interactie tussen melder en meldpunt plaatsvindt, omdat het risico van valse meldingen, zwartmakingen en witwassen van informatie door de politie groter is bij eenrichtingsconstructies als een webformulier dan bij tweerichtingsverkeer als een chatmodaliteit.

Hoofdstuk 6

Organisatorische aspecten

Zoals we in hoofdstuk 4 hebben gezien geeft de technische inrichting van een Internet gebaseerd meldpunt grote invloed op de anonimiteit van de melder en de meldingen, alsmede de kwaliteit van de uiteindelijke meldingen die doorgegeven worden aan de afnemers. Maar niet alleen de techniek is van belang: ook de organisatorische inrichting van het meldpunt speelt een rol. In dit hoofdstuk gaan we hier kort op in. De organisatorische analyse is beduidend minder diepgaand dan de technische, juridische en normatieve analyse. Dit is gelegen in het feit dat de relevante organisatorische issues die invloed hebben op een Internet gebaseerd meldpunt niet wezenlijk anders zijn dan de issues die invloed hebben op een telefonisch meldpunt. We beschrijven hier daarom enkel de relevante verschillen.

Het waarborgen van de anonimiteit van de melder en de meldingen is een onderdeel van het in algemene zin garanderen van de veiligheid van het ingerichte meldpunt. Hiervoor is een goede keuze voor een technische inrichting een noodzakelijke maar niet voldoende voorwaarde. Juist het operationeel beheer over het systeem is van cruciaal belang om de veiligheid te garanderen gedurende de vele jaren dat het systeem operationeel zal zijn.

6.1 Institutionele inbedding

Zoals al in een eerder hoofdstuk is beargumenteerd (ondermeer paragraaf 3.4) heeft de keuze om het telefonisch meldpunt onder te brengen bij een private partij (in casu Stichting M.) bepaalde consequenties. Het is dus van belang de keuze voor een publieke dan wel private inrichting van het Internetmeldpunt op basis van weloverwogen argumenten te maken. De keuze voor een private partij betekent dat publieke waarden zoals de rechtsbescherming e.a. op een andere manier beschermd moeten worden, en dat de overheid hierop strak moet toezien.

6.2 Beheer

Een fundamentele keuze die het meldpunt hierin moet maken is de vraag of zij het beheer over de technische inrichting in eigen beheer uitvoert (als zij zelf fysiek de inrichting onder haar hoede heeft, zie 4.2.3), of uitbesteedt aan een derde partij.

In het eerste geval is het van groot belang dat het systeembeheer de juiste kennis en kwaliteiten in huis heeft om een dergelijk systeem te beheren en onderhouden. Het is belangrijk daarin te onderkennen dat het systeem speciaal voor het meldpunt zal zijn ontworpen, waardoor er qua beheer nog geen ervaring is opgedaan in eerdere situaties. Daarnaast stelt het systeem, vanwege de aard van haar functie specifieke eisen aan het beheer om de veiligheid, en dan specifiek de anonimiteit, te garanderen. Belangrijk is in deze context bijvoorbeeld de vraag hoe men omgaat met het vernietigen van meldingen en daaraan gerelateerde data, en andere informatie die het systeem gedurende het verwerken van meldingen bewaart.

Kiest het meldpunt ervoor om het beheer onder te brengen bij een derde partij (wat ook mogelijk is als het systeem zelf binnen de muren van het meldpunt is gesitueerd), dan is het van groot belang duidelijke afspraken over het beheer, en de garanties die de beherende partij hier op geeft, vast te leggen in een zogenaamde Service Level Agreement (SLA).

Welke keuzes hierin ook gemaakt worden, het is belangrijk dat helder is wie verantwoordelijk is voor de technische waarborging van de anonimiteit.

Zoals ook al eerder is opgemerkt (hoofdstuk 2) heeft Stichting M. voor het telefonisch meldpunt zowel de computersystemen als de telefonie geoutsourced aan Pink Elephant [25]. Hierbij wordt zelfs de mogelijkheid geboden voor medewerkers om thuis te werken. Deze benadering is in onze ogen risicovol.

6.3 Audits

Onafhankelijk van de keuze voor uitbesteden dan wel beheer in eigen beheer dient het systeem regelmatig geaudit te worden. Dergelijke audits dienen door een gekwalificeerde externe partij uitgevoerd te worden. Deze audit moet de hele keten van het meldproces, inclusief het beheer en de organisatie, bestrijken. Juiste de koppeling met de afnemers van de meldingen (op dit moment via Meldnet) en de manier waarop een melding 'aan de voorkant' binnenkomt hebben grote invloed op de veiligheid en betrouwbaarheid van het systeem. Ook de expertmeeting onderschreef de noodzaak van zulke audits.

6.4 Personeel en werkomgeving

Integriteit van de personele bezetting van het meldpunt is van cruciaal belang. Het meldpunt Kinderporno screent bijvoorbeeld alle nieuwe medewerkers en traint deze intern. Het is verboden eigen apparatuur mee te nemen naar het meldpunt, en er wordt gewerkt met vaste werkstations (geen laptops). Het meldpunt kinderporno heeft er voor gekozen deze werkstations zelf door het eigen systeembeheer te laten onderhouden. Schoonmakers, tenslotte, zijn alleen welkom als er ook reguliere medewerkers aanwezig zijn.

6.5 Kosten/baten analyse

Een belangrijke afweging in de keuze al dan niet een Internetmeldpunt in te richten is de vraag hoeveel de noodzakelijke investering in zo'n meldpunt oplevert.

Zowel over de kosten als over de baten is slechts in algemene zin iets te zeggen. Uit de technische analyse in hoofdstuk 4 volgt dat een Internetmeldpunt niet met een standaard software pakket ingericht kan worden. Het gaat om een apart te ontwikkelen systeem dat aan hoge anonimiteitseisen moet voldoen. De verwachting is dan ook dat de ontwikkel- en beheerskosten hoog zullen zijn. Cijfers uit andere landen zijn vanwege de fundamenteel andere insteek van meldpunten aldaar (zie 4.7) niet echt maatgevend.

De te verwachten opbrengsten zijn zo mogelijk nog lastiger in te schatten, zoals al eerder op verschillende plekken in dit rapport is opgemerkt. De verwachting heerst dat een Internetmeldpunt tot veel meer anonieme meldingen kan leiden. De specifieke inrichting van een Internetmeldpunt is echter van grote invloed op de bruikbaarheid van de meldingen. Tenslotte heeft een mogelijke toename van het aantal meldingen en een andere kwaliteit van die meldingen weer zijn invloed op het gebruik van die meldingen bij de opsporing en in het strafrechtelijke proces, wat mogelijk tot minder (in plaats van meer) succesvolle strafzaken kan leiden.

6.6 Invoeringsstrategie

Op dit moment is er enige onduidelijkheid over de kwaliteit van de meldingen en daarmee over de effectiviteit van het meldpunt (zie 2.1). Zo zijn alleen cijfers bekend over het gebruik van meldingen bij de politie, en niet voor de overige afnemers. Voor een verantwoorde invoering van Internet als een nieuw kanaal zou het goed zijn als een gedegen en breed gedragen analyse van de effectiviteit van het huidige telefonische meldpunt beschikbaar is. Tegen deze baseline kan vervolgens de effectiviteit van het Internet als nieuw kanaal vervolgens afgezet worden. Op basis van deze gegevens kunnen vervolgens goed onderbouwde beslissingen genomen worden over het uitbouwen dan wel terugschroeven van het Internet als meldkanaal.

Onafhankelijk hiervan verdient het aanbeveling om het Internet als nieuw kanaal geleidelijk in te voeren, bijvoorbeeld door deze te beperken tot het melden van bepaalde vormen van misdaad. Het is belangrijk de mogelijkheid te hebben een stap terug te doen als blijkt dat het kanaal niet voldoet (in termen van anonimiteit, kwaliteit en effectiviteit).

In de expertmeeting werd nog de parallel getrokken met de oprichting van 112 en de hausse van meldingen die deze dienst in het begin te verwerken kreeg: die ebde na 3 maanden weg. Het is van belang om dit in het achterhoofd te houden als na het openen van een Internetmeldpunt een vergelijkbare sprong in meldingen optreedt. Er moet niet te snel aan de noodrem getrokken worden.

Hoofdstuk 7

Conclusies

In ons onderzoek hebben wij gepoogd antwoord te krijgen op de vraag of het technisch, juridisch en organisatorisch mogelijk is om de anonimiteit van melders te garanderen bij meldingen via Internet. Daarnaast hebben wij onderzocht wat de mogelijke voor- en nadelen van melden via Internet zijn voor (1) de hoeveelheid en kwaliteit van de meldingen en (2) voor de rol die deze meldingen spelen in de strafvordering en in het maatschappelijk verkeer. Omdat het hier een quickscan betreft zijn de antwoorden vrij algemeen van aard, en heeft het onderzoek vooral een aantal nieuwe vragen voor diepgaander onderzoek opgeleverd. Desalniettemin zijn er in grote lijnen een aantal relevante conclusies te trekken. Deze zijn geordend volgens de oorspronkelijke onderzoeksvragen (zie voor de subvragen paragraaf 1.1.1):

1. In hoeverre is het haalbaar om de anonimiteit van melders te garanderen bij meldingen via Internet, vanuit technisch, juridisch en organisatorisch perspectief?
2. Welke zijn, op technisch, juridisch en organisatorisch vlak, de mogelijke of verwachte voor- en nadelen van anoniem melden via Internet?

7.1 Haalbaarheid garanderen anonimiteit Internetmeldpunt

Ten aanzien van de haalbaarheid om de anonimiteit van melders te garanderen bij meldingen via Internet zijn de volgende conclusies te trekken.

Een technisch voldoende veilige inrichting van een Internetmeldpunt is geen sinecure. Een aantal verschillende partijen heeft belang bij, en de mogelijkheid om, de identiteit van een melder te achterhalen. Denk hierbij aan personen in de directe omgeving van de melder, personen en (criminele) organisaties die het onderwerp zijn van meldingen, en ook de opsporingsdiensten.

Over de mogelijke technische inrichting van een Internetmeldpunt, de mate van bescherming die deze biedt en de mogelijke nadelen die daar aan verbonden zijn, concluderen wij het volgende. Vanuit technisch perspectief is er een duidelijk verschil tussen een Internetmeldpunt en een telefonisch meldpunt. Vanwege het open karakter van het Internet is het lastig om de communicatie tussen melder en meldpunt anoniem (i.e. onobserveerbaar) te maken. Anonimimiseringssoftware zoals Tor kan hier in theorie tegen beschermen maar is in de praktijk te complex om voor de gemiddelde gebruiker te adviseren. Dat betekent dat de anonimiteit van de melder niet voldoende gegarandeerd kan worden. Daarnaast zal een gemiddelde gebruiker ongewild sporen achterlaten, en is ook de vernietiging van gegevens aan de kant van het meldpunt een punt van zorg. Interactiviteit tussen melder en meldpunt is essentieel voor een kwalitatief goede en voldoende anonieme melding. Van alle geïdentificeerde oplossingsrichtingen (we verwijzen hiervoor naar paragraaf 4.8) voldoet een web-gebaseerde chat toepassing of een smartphone app nog het meest aan de gestelde eisen. Maar ook hier is de technische complexiteit hoog en is, zoals hierboven al gezegd, de garantie van anonimiteit sub-optimaal. Vanwege de hoge complexiteit verwachten wij dat de kosten voor het inrichten van zo'n Internetmeldpunt ook hoog zullen zijn. Concrete cijfers zijn hier echter nier over te geven, vanwege het gebrek aan vergelijkbare systemen.

Vanuit juridisch perspectief is het verschil tussen Internetmeldpunt en een telefonisch meldpunt minder groot. De Wet bescherming persoonsgegevens vormt geen belemmering. We verwachten dat de verwerking van persoonsgegevens door een Internetmeldpunt even rechtmatig is als bij het telefonisch meldpunt. De Wet bewaarplicht telecommunicatiegegevens vormt enkel een risico voor een Internetmeldpunt op basis van e-mail. Alleen voor e-mail legt de wet een bewaarplicht van 6 maanden op t.a.v. gegevens over wie met wie communiceert. Het onderscheppen van communicatie (het 'tappen') door opsporingsdiensten is een risico voor een Internetmeldpunt, omdat een technische voorziening om dit ten aanzien van het meldpunt te voorkomen lastiger lijkt te organiseren voor een Internettap dan voor een telefonische tap. Wat betreft

aansprakelijkheidsrisico's zien wij geen noemenswaardige verschillen tussen een Internetmeldpunt en een telefonisch meldpunt. Wel ligt het aansprakelijkheidsrisico bij een door een private partij ingericht meldpunt hoger. Een goede maatregel zou zijn om de Instructie Meld Misdaad Anoniem van het College van Procureurs-Generaal zou ook van toepassing te laten zijn voor een Internetmeldpunt, en op alle vormen van opsporingsonderzoek, inclusief doorzoeking en het vorderen van gegevens.

In organisatorische zin is het grootste verschil tussen een Internetmeldpunt en een telefonisch meldpunt, dat de verhoogde technische complexiteit van een Internetmeldpunt een hoger kennisniveau van de hele organisatie vereist. Beheer wordt complexer, en als de infrastructuur geoutsourced wordt is juist het toezicht hierop complexer. Regelmatige audits zijn een essentiële maatregel om de anonimiteit te blijven garanderen.

Als we kijken naar de combinatie van technische, juridische en organisatorische mogelijkheden en obstakels voor de anonimiteit van meldingen via Internet, dan valt op dat vooral de technische inrichting van een meldpunt dat de anonimiteit van de melder afdoende beschermd een uitdaging is.

7.2 Voor- en nadelen van een Internetmeldpunt

Ten aanzien van de mogelijke of verwachte voor- en nadelen van anoniem melden via Internet zijn de volgende conclusies te trekken.

Over de te verwachten hoeveelheid meldingen die via een Internetmeldpunt binnen kunnen komen is weinig te zeggen. Vergelijkbare interactieve systemen zoals we die in dit rapport voorstaan en die dezelfde mate van anonimiteit garanderen zijn nog niet eerder ontwikkeld en in de praktijk toegepast.

Ten aanzien van de kwaliteit van de meldingen geldt dat de inrichting van het Internetmeldpunt hierop van grote invloed is. Zoals hierboven reeds vermeld geldt voor de technische inrichting dat interactiviteit tussen melder en meldpunt essentieel is voor een kwalitatief goede en voldoende anonieme melding. Als er voor een dergelijke inrichting van een Internetmeldpunt gekozen wordt verwachten wij geen daling van de kwaliteit van de meldingen.

Over de rol van anonieme meldingen in de opsporing legt onze analyse bloot dat een laagdrempelig Internetmeldpunt tot ongewenste neveneffecten kan leiden. Te denken valt aan schadeclaims en onrechtmatigedaadsacties tegen de overheid, of dat de rechter vanwege de lage kwaliteit van de meldingen zwaarder invulling kan gaan geven aan het criterium van aanvullende informatie.

Ten aanzien van de rol van anonieme meldingen in het maatschappelijk verkeer blijkt uit de normatieve analyse dat er een risico bestaat bij een meldpunt van function creep, zowel voor wat betreft het type misstanden dat wordt gemeld als voor het gebruik buiten de opsporing van anonieme meldingen die in politiebestanden terechtkomen. In een klimaat waarin politiële databanken op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet, is het belangrijk om terughoudend te zijn met het voeden van politiële databanken met ongecontroleerde informatie. Dit pleit voor terughoudendheid bij het faciliteren van anonieme meldingen.

7.3 Overwegingen

Onze quickscan heeft, naast bovenstaande conclusies, ook een aantal onzekerheden en meer fundamentele vragen naar boven gebracht. Veel is nog onduidelijk, vooral wat betreft de kosten en het aantal te verwachten meldingen via een Internetmeldpunt. Nadere studie ter beantwoording daarvan is gewenst voordat onomkeerbare stappen in de richting van een Internetmeldpunt worden gezet. We willen de volgende overwegingen graag aan de lezer meegeven.

- Om de meerwaarde van een Internetmeldpunt objectief te kunnen vergelijken met de huidige situatie, is het aan te raden een onafhankelijke en breed gedragen nulmeting te doen aangaande de kwaliteit en bruikbaarheid van de meldingen die het telefonisch meldpunt oplevert. Bestaand onderzoek over de kwaliteit van de meldingen van het bestaande telefonisch meldpunt is beperkt tot de bijdragen aan het werk van de politiële opsporing, en wordt betwist door het meldpunt.
- Nader onderzoek naar een specifieke inrichting van een Internetmeldpunt, met een risicoanalyse die dieper gaat dan in het bestek van deze quickscan gemaakt kon worden, vinden wij gewenst. Hierbij zou ook een onderzoek naar de te verwachten kosten meegenomen moeten worden.
- Gezien het risico van function creep bij een Internetmeldpunt is eerst een bredere reflectie nodig op de vraag voor welk soort meldingen een anoniem meldpunt bedoeld is en of het wenselijk is dat meldingen ter beschikking worden gesteld aan derden en ook gebruikt worden voor doeleinden buiten de opsporing en vervolging van strafbare feiten. Gestreefd zou moeten worden naar het opstellen van een proportionaliteitstoets dienaangaande.

- Daarnaast zou ook beargumenteerd moeten worden of een Internetmeldpunt door een publieke dan wel private partij ingericht moet worden.
- Tenslotte lijkt het ons inziens verstandig om, als de vraag of een Internetmeldpunt überhaupt wenselijk is positief is beantwoord, eerst met een beperkte pilot te beginnen om de animo voor een Internetmeldpunt beter in te kunnen schatten.

Bibliografie

[1] Kai Biermann. http://blog.zeit.de/open-data/2012/07/30/daten-technik/ bezocht op 5 januari 2014.

[2] Blauw Research: *Evaluatie pilot Meld Misdaad Anoniem. Eindrapportage*. Blauw Research, Rotterdam, 2003.

[3] S. Boes: *M. van A tot Z: een analyse van Stichting M. als voorziening tot burgerparticipatie op het gebied van sociale veiligheid*. Masterscriptie criminologie, Universiteit Leiden, Maart 2010.

[4] Frank Bongers, Rudi Bekkers, Tommy van der Vorst, Reg Brennenraedts, en David van Kerkhof: *Vooronderzoek evaluatie van automatische nummerherkenning geheimhoudergesprekken advocatuur*. Dialogic/WODC, 2013.

[5] S. Brinkhoff: *Anoniem melden startinformatie voor een strafrechtelijk onderzoek?* Nederlands Juristenblad, 83(20):1224–1228, 2008.

[6] Y. Buruma: *Ongemakkelijke lessen van Lucia*. Delikt en Delinkwent, 40(6):689–706, Juni 2010.

[7] Y. Buruma: *Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld*. In D. Broeders, C.M.K.C. Cuijpers, en J.E.J. Prins (redactie): *De staat van informatie*, pagina's 165–221, Amsterdam, 2011. Amsterdam University Press.

[8] College Bescherming Persoonsgegevens: *Brief aan stichting meld misdaad anoniem*. 14 juli 2005, kenmerk z2005-0074, 2005.

[9] College van Procureurs-Generaal: *Instructie meld misdaad anoniem*. 10 april 2006, registratienummer 2006I007, 2006.

[10] Alexei Czeskis, David Mah, Omar Sandoval, Ian Smith, Karl Koscher, Jacob Appelbaum, Tadayoshi Kohno, en Bruce Schneier: *Deaddrop/strongdrop security assessment*. Technisch Rapport UW-CSE-13-08-02, University of Washington, 2013.

[11] W. Dreissen en O. Nauta: *Anonimiteit in het strafproces. De praktijk van de regeling beperkt anonieme getuige en de regeling bedreigd anonieme getuige in het strafproces*. DSP-groep/WODC, Amsterdam, 2012.

[12] D. Garé: *Het blijft tobben met de anonieme getuige*. Nederlands Juristenblad, 36:1636–1640, 1998.

[13] GlobalLeaks: *Globaleaks application security design and details*. https://docs.google.com/document/d/1SMSiAry7x5XY9nY8GAejJD75NWg7bp7M1PwXSiwy62U/pub bezocht op 14 februari 2014, versie: "Updated to software release 2.54, February 2014".

[14] GlobalLeaks: *Globaleaks threat model and security design*. https://docs.google.com/document/d/1niYFyEar1FUmStC03OidYAIfVJf18ErUFwSWCmWBhcA/pub bezocht op 14 februari 2014, versie: "Release 0.2 of June 2013 (last update, Jan 2014)".

[15] Ian Goldberg en Others: *Off-the-Record Messaging*. https://otr.cypherpunks.ca/index.php bezocht 19 januari 2014.

[16] B. Hoogenboom en E. Muller: *Voorbij de dogmatiek: publiek-private samenwerking in de veiligheidszorg*. Kerckebosch, Zeist, 2002.

[17] F. van Kolfschooten: *Alles wat jurist is in mij, komt in opstand tegen anonieme klachten*. NRC Handelsblad 8 februari 2014, pagina W8, 2014.

[18] B.J. Koops en J.M. Smits, m.m.v. F. van der Kroon: *Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie*. Wolf Legal Publishers, Oisterwijk, 2014.

[19] M. van Kuik, S. Boes, N. Kop, en M. den Hengst-Bruggeling: *M.-waarde*. Politie & Wetenschap, 2012.

[20] Tom Lazar: *Briefkasten*. https://github.com/ZeitOnline/briefkasten bezocht op 5 januari 2014.

[21] E. Lissenberg: *Klokkenluiders en verklikkers*. Afscheidsrede Amsterdam (UvA), 15 februari, 2008.

[22] J. Mazzone en T. Fischer: *The normalization of anonymous testimony*. In *Secrecy, National Security and the Vindication of Constitutional Law*, pagina's 195–208, Cheltenham, UK, 2013. Edward Elgar.

[23] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Veiligheid en Justitie: *Veilige publieke taak en (gedeeltelijke) anonimiteit in het strafproces*. Factsheet, 2013. http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2013/08/13/factsheet-veilige-publieke-taak-en-gedeeltelijke-anonimi

teit-in-het-strafproces.html.
[24] Article 29 Data Protection Working Party: *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf. WP211, 27 February 2014.
[25] Pink Elephant: *Customer case: Stichting m*.
[26] H. Schnitzler: *We leven in een "klikspaan boterspaan"-land*. De Volkskrant 22 februari, 2012.
[27] Secure Drop: *User manual*. https://github.com/freedomofpress/securedrop/blob/master/docs/user_manual.md bezocht 5 januari 2014.
[28] R. van Steden: *Voorbij de dogmatiek: publiek-private samenwerking in de veiligheidszorg. boekbespreking*. Openbaar bestuur, pagina 30, Augustus 2003.
[29] Stichting NL Confidential. Persoonlijke mededeling, 9 januari, 2014.
[30] TipSoft: *Tipsubmit mobile*. http://www.tipsoft.com/TipSubmitMobile.pdf.
[31] TipSoft: *Webtips*. http://www.tipsubmit.com/AccMan/uploads/tipsoft.com/TipSoft%20WebTips.pdf.
[32] Veiligezorg: *handreiking aangifte doen bij de politie*, 2013. http://www.veiligezorg.nl/kenniscentrum/bestand-informatie/handreiking_aangifte_20131001.
[33] Julien Voisin, Christophe Guyeux, en Jacques M. Bahi: *The metadata anonymization toolkit*. CoRR, abs/1212.3648, 2012.
[34] Wetenschappelijke Raad voor het Regeringsbeleid: *Het borgen van publiek belang*, 2000.

Bijlage A

Verklarende Woordenlijst

DNS Domain Name System
IM Instant Messaging
IP Internet Protocol
ISP Internet Service provider
SSL Secure Socket Layer, opgevolgd door TLS
TLS Transport Layer Security, de opvolger van SSL
VoIP Voice over IP
VPN Virtual Private Network

Bijlage B

Begeleidingscommissie

De begeleidingscommissie voor dit rapport bestond uit de volgende personen

- dr. F.W. (Frans) Beijaard, WODC.
- S. (Sanne) Boes, MSc, NHL Hogeschool en Politieacademie.
- prof. dr. N.A.N.M. (Nico) van Eijk, Universiteit van Amsterdam (voorzitter).
- mr. ir. A.P. (Arnout) Engelfriet, Vrije Universiteit & ICT Recht.
- T. (Timo) Hilbrink, XS4ALL.
- drs. T. (Tim) Veenings, Ministerie van Veiligheid en Justitie.

De onderzoekers bedanken de leden van de begeleidingscommissie voor de waardevolle discussies en hun constructieve commentaar op eerdere versies van dit onderzoeksrapport.

Bijlage C

Deelnemers expert workshop

De volgende personen hebben deelgenomen aan de expert workshop op vrijdag 31 januari 2014.

- Warner de Boer, Politie Oost-Nederland.
- Sanne Boes, NHL Hogeschool en Politieacademie.
- Timo Hilbrink, XS4ALL Techteam.
- Matthijs Koot, Madison Gurkha.
- Wim Michels, Politie Oost-Nederland.
- Maaike Pekelharing, Meldpunt Kinderporno op Internet.
- Bas de Wilde, Vrije Universiteit Amsterdam.

Wij zijn hen zeer erkentelijk voor hun bijdrage aan deze workshop.

Daarnaast namen de drie auteurs van dit rapport deel aan de expert workshop.