



Haalbaarheid van een anoniem misdaadmeldpunt via het Internet

Een quickscan

Samenvatting

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.

© 2014; Wetenschappelijk Onderzoek - en Documentatiecentrum (WODC). Auteursrechten voorbehouden. Niets uit dit rapport mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, digitale verwerking of anderszins, zonder voorafgaande schriftelijke toestemming van het WODC.

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 politiebesteden terecht komen. 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 politieke databanken op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet, is het belangrijk om terughoudend te zijn met het voeden van politieke databanken met ongecontroleerde informatie. Dit pleit voor terughoudendheid bij het faciliteren van anonieme meldingen.