Universiteit Utrecht

Methodenonderzoek Dark number jeugdige daders in Nederland van gedigitaliseerde criminaliteit en cybercriminaliteit

(Samenvatting, conclusies, aanbevelingen)

Peter G.M. van der Heijden (Universiteit Utrecht)
Maarten J.L.F. Cruyff (Universiteit Utrecht)
Ger H.C. van Gils (BeleidsOnderzoek&Advies (BOA))
Utrecht, september 2017

Samenvatting, conclusies, aanbevelingen

1. Inleiding

Dit rapport is een verslag van een onderzoek naar een aantal methoden om de omvang van online delicten, in het bijzonder onder jeugdigen te schatten. Het gaat om de vraag of er methoden zijn die verbeteringen of aanvullingen van de aanpak van de Monitor Jeugdcriminaliteit 2015 kunnen opleveren. Deze is gebaseerd op (1) zelfrapportage van respondenten met directe vragen (de 5-jaarlijkse Monitor Zelfrapportage Jeugd (MZJ)) en (2) data uit de strafrechtketen. Innovatieve technieken stonden in dit onderzoek met nadruk op de agenda.

De onderzoeksvraag luidde: met welke onderzoeksmethode of (combinatie van) methoden kan, voortbouwend op de inzichten uit de Monitor Jeugdcriminaliteit 2015 (MJC), het percentage jeugdigen in Nederland worden geschat dat zich schuldig maakt aan de volgende misdrijven:
(1) online bedreiging,
(2) het online verspreiden van seksueel beeldmateriaal van minderjarigen en
(3) het inloggen op een computer/website zonder toestemming/kennisgeving, al dan niet gepaard met het wijzigen van gegevens.

Onder 'jeugdigen' wordt verstaan personen vanaf 12 tot en met 22 jaar oud.

Op basis van een eerste verkenning in het onderzoeksvoorstel zijn vier methoden geselecteerd voor nader onderzoek. Het betreft twee methoden om gegevens met vragenlijsten bij respondenten te verzamelen, te weten de Network Scale Up Method en randomized response en twee methoden die gebruik maken van reeds beschikbare data.
De methoden zijn in de eerste plaats beoordeeld op de vraag of er betrouwbare en valide schattingen van de omvang van moeilijk toegankelijke populaties, zogenaamde 'dark numbers', mee zijn te maken. Deze vraag verdient een uitgebreide beantwoording in het geval van de twee methoden waarmee nog weinig tot geen ervaring bestaat in grootschalig toegepast onderzoek, de Network Scale-Up Method (NSUM) en Social Media Tekst Profiling (SMTP). Bij de twee andere methoden, randomized response en vangst-hervangst, die al tot het standaardarsenaal van beleidsondersteunend onderzoek behoren, spitst de beoordeling zich toe op meer praktische vragen. In het geval van randomized response gaat het om de vraag of de techniek betere resultaten oplevert dan directe bevraging zoals gebruikt in de MZJ. Bij vangst-hervangst is de beschikbaarheid van voldoende data uit de politieregistratie het belangrijkste criterium.
Voor alle methoden wordt nagegaan welke typen vragen er mee zijn te beantwoorden, bijvoorbeeld vragen naar modus operandi en daderkenmerken en of er bijzonderheden gelden bij onderzoek naar online delicten en bij onderzoek onder jeugdigen. Verder is er ook aandacht geschonken aan te verwachten kosten van gebruik van gebruik van de methoden, en, waar van toepassing, aan de verkrijgbaarheid van data.

In de navolgende paragrafen vatten we de belangrijkste bevindingen over de vier methoden uit het onderzoek kort samen, trekken we conclusies over de bijdragen die de methoden kunnen leveren aan het maken van een schatting van online criminaliteit. Op basis van die conclusies doen we

aanbevelingen voor mogelijke vervolgacties. De slotparagraaf geeft de belangrijkste conclusies en aanbevelingen over de vier verschillende methoden kort en in samenhang weer.

2. Network Scale Up Method (NSUM)

Met NSUM wordt respondenten in een survey gevraagd om de aantallen mensen te tellen die zij kennen inde subpopulatie waarvan de omvang geschat moet worden. Daarnaast wordt gevraagd naar aantallen contacten in een aantal subpopulaties van bekende omvang. Met die gegevens kan de omvang van het netwerk van de respondenten worden geschat en de omvang van de subpopulaties die nog niet bekend waren. Omdat niet naar het gedrag van de respondent zelf wordt gevraagd, is de veronderstelling dat er een betere, minder sociaal wenselijke rapportage uit volgt van zaken die mogelijk gevoelig liggen.

Conclusies over (potentiële) opbrengst

NSUM beoordelen wij als een interessante methode om de omvang van moeilijk toegankelijke populaties te schatten. De methode maakt het voor respondenten waarschijnlijk makkelijker om over deviant gedrag te rapporteren. De ervaring met NSUM in grootschalige surveys en bevolkingsonderzoek is echter nog beperkt. Ook zijn we geen gedegen validatie-onderzoek tegen gekomen waarin een vergelijking wordt gemaakt met andere methoden. De bestudeerde literatuur vermeldt geen ervaringen met onderzoek van online criminaliteit of onder jongeren. Er zijn weinig redenen om voor onderzoek onder jongeren bijzonderheden te veronderstellen. Bij delicten die in beginsel makkelijk alleen zijn te plegen en waarover in een sociale kring weinig bekend is, werkt de methode niet goed. Computervredebreuk is daar mogelijk een voorbeeld van.
Positief is dat de methode betrekkelijk eenvoudig en zonder veel bijkomende kosten en voorzieningen in een enquête is op te nemen. Er zijn geen grotere steekproeven nodig dan bij gewone enquêtes. Wel zullen de vragenlijsten iets langer worden, de enquêtetijd zal toenemen en de constructie van de vragenlijst vereist extra tijd en aandacht omdat het vragen naar subpopulaties van bekende omvang een zorgvuldige voorbereiding en selectie vergt. Bij onderzoek naar online delicten dient aandacht te worden geschonken aan de vraag hoe een relevant en reëel bestaand netwerk van respondenten op social media kan worden gedefinieerd.

We concluderen dat de NSUM voldoende perspectief biedt om informatie te leveren over de prevalentie van online delicten. De informatie die ermee kan worden verkregen, is waarschijnlijk beperkter dan met de andere enquêtemethoden zoals directe bevraging en randomized response is te verkrijgen. We kunnen er immers niet vanuit gaan dat respondenten volledig op de hoogte zijn van het wel en wee van iedereen in hun sociale kring. Het gegeven waarnaar gevraagd kan worden is waarschijnlijk beperkt tot het daderschap en mogelijk enkele eenvoudig vast te stellen kenmerken van daders en delicten. Een vraag of een delict bijvoorbeeld een buitenlands slachtoffer heeft, voert waarschijnlijk te ver.

Aanbevelingen

Een eerste te overwegen stap om meer inzicht in de mogelijkheden van de methode te krijgen is het uitvoeren van een simulatiestudie. In zo'n studie wordt de methode toegepast op een (zelf gegenereerde) populatie waarvan alle eigenschappen volledig bekend zijn. Op deze manier kan op korte termijn, met beperkte middelen en op gecontroleerde wijze de betrouwbaarheid van NSUM

schattingen worden getoetst. Daarnaast is het ook mogelijk om de invloed van het schenden van de belangrijkste veronderstellingen van de methode te bepalen en van maatregelen om die invloed te beperken.

Verder denken we dat het te overwegen is om een validatiestudie van NSUM uit te voeren, bijvoorbeeld in de vorm van een vergelijking met een schatting op basis van directe bevraging. Dat kan door vergelijking van de uitkomsten van een onderzoek met NSUM met cijfers uit de MZJ. Maar beter is de twee onderzoeksmethoden onder zoveel mogelijk gelijke condities te gebruiken. Dat zou tegen betrekkelijk beperkte kosten kunnen in bijvoorbeeld een internetpanel. We veronderstellen dan dat eventuele verschillen tussen de methoden niet anders uitvallen bij gebruik van verschillende kanalen, i.c. een internetpanel en face-to-face benadering.

De literatuur maakt duidelijk dat er mogelijkheden zijn om het gebruik van de methode te optimaliseren. De voorgestelde maatregelen inzake databewerking kunnen eenvoudig allemaal worden uitgeprobeerd op reeds beschikbare data van NSUM-onderzoek of op gegeneerde data in een simulatiestudie. De meest interessante voorzieningen voor dataverzameling kunnen in een validatieonderzoek worden uitgeprobeerd.

Tot slot, de literatuur over NSUM bevat geen aanwijzingen voor beantwoording van de vraag hoe rekening te houden met het ‘virtuele’ netwerk van respondenten op social media. Het is van belang om voor een enquête waarin van NSUM gebruik wordt gemaakt, deze vraag te beantwoorden, bijvoorbeeld aan de hand van recente literatuur over sociale netwerken of van bestaande enquêtes onder gebruikers van social media.

3. Randomized response

Ook Randomized response is een methode om vragen te stellen over gevoelige zaken waarbij respondenten ertoe neigen ze verborgen te houden. Het is inmiddels een betrekkelijk bekende en vertrouwde methode. Het antwoord van de respondent kan op verschillende manieren, bijvoorbeeld met een worp met dobbelstenen, met een kans worden ‘vermengd’, waardoor het ware antwoord van elke afzonderlijke respondent niet meer is te achterhalen, maar op basis van de bekende kansverdeling voor de hele groep wel is te schatten. Randomized response biedt daarom in vergelijking met directe bevraging extra bescherming van anonimiteit voor respondenten bij onderwerpen die gevoelig liggen, tegen de kostprijs van een (mogelijk aanzienlijk) grotere steekproef. De methode is gebruikt voor o.m. het schatten van het voorkomen van sociale zekerheidsfraude, diefstal in de zorg en dopinggebruik in de sport.

Conclusies over (potentiële) opbrengst

Met Randomized response kunnen in principe dezelfde gegevens over delicten worden verzameld als met gewone directe bevraging zoals die bijvoorbeeld in de MZJ wordt gebezigd. Dat betekent dat er weinig beperkingen zijn ten aanzien van de informatie die kan worden verkregen. De vragenlijst van een onderzoek kan betrekkelijk flexibel op de informatiebehoefte worden afgestemd. Er kunnen vragen worden gesteld over daderschap, manieren waarop men te werk is gegaan, de motivatie en eventuele opbrengst van de delicten, eventuele slachtoffers in het buitenland, etc. Vragen naar heel specifieke gedragingen of kenmerken kunnen extra bedreigend zijn voor respondenten. Bovendien wordt de kans kleiner dat men significante aantallen respondenten in een steekproef aantreft die aan het gevraagde kenmerk voldoen. Dat zijn óverigens beperkingen van elke vorm van (vragenlijst)onderzoek.

Het is ook mogelijk om statistische relaties te leggen tussen verschillende groepskenmerken, bijvoorbeeld het toegeven van een delict enerzijds en geslacht, leeftijd of opleiding anderzijds. Vooralsnog moet een voorbehoud worden gemaakt ten aanzien van het bevragen van de exacte frequentie waarmee een delict in een bepaalde periode is begaan. Deze specifieke techniek zou eerst verder moeten worden ontwikkeld. Wel zijn er goede ervaringen opgedaan met het vragen naar frequentieklassen (“heeft u het nooit/1-3 keer/ . . ./meer dan 12 keer gedaan?”).

Er zijn geen aanwijzingen dat er bijzondere problemen of uitdagingen te verwachten zijn bij onderzoek met randomized response naar online delicten of onder jongeren.

Een belangrijke overweging bij de keuze van randomized response is de omvang van de benodigde steekproeven. Om informatie te verkrijgen die vergelijkbaar is met de MZJ zou mogelijk een steekproef van 10.000 respondenten voor een van de leeftijdscategorieën moeten worden gerealiseerd, een onmogelijke opgave. Bij gebruik van vervolgvragen neemt de vereiste omvang van de steekproef substantieel af. Niettemin is te verwachten dat gebruik van randomized response in de MZJ een majeure ingreep zal betekenen en tot een duidelijke verhoging van de kosten zal leiden. Het is niet bekend of jeugdigen er veel moeite mee hebben om het begaan van delicten, online dan wel offline, toe te geven. Het zou daarom voorbarig zijn om voor te stellen randomized in te zetten voor de MZJ.

Aanbevelingen

Een vergelijkend onderzoek van randomized response met conventionele directe bevraging kan bepalen of er sprake is van onderrapportage van online delicten door jeugdigen en hoe groot of ernstig eventuele onderrapportage is. In zo’n onderzoek worden dezelfde vragen over online delicten direct en met randomized response aan twee verschillende groepen respondenten uit dezelfde populatie voorgelegd.

Op basis van de resultaten kan worden besloten randomized response al of niet op te nemen in de MZJ. Een alternatief kan zijn de vinger aan de pols te houden door met enige regelmaat de vergelijking van randomized response met directe vragen te maken.

Om de kosten van zo’n onderzoek in de hand te houden, kan het onderzoek worden opgenomen in een internetpanel. Mogelijk kan worden volstaan met een beperkt aantal vragen in een ‘omnibusconstructie’ waar meerdere kleine onderzoeken zijn opgenomen. Overigens gaan we er bij een vergelijking via een internetpanel vanuit dat een eventueel verschil tussen directe bevraging en randomized response in een internetpanel niet anders uitvalt dan in een face-to-face enquête.

Ook is het mogelijk om de vergelijking de eerste keer grofmazig op te zetten, bijvoorbeeld alleen voor het delict met de hoogste prevalentie. Het onderzoek heeft dan alleen het doel te onderzoeken of jeugdigen in het algemeen anders reageren op de verschillende methoden.
Een andere mogelijkheid om op de kosten te besparen is door alleen verschillen te toetsen tussen de rapportage van groepen delicten, bijvoorbeeld de gedigitaliseerde delicten tezamen. Als randomized response inderdaad een significant hogere rapportage oplevert, voldoen bij vervolgonderzoek kleinere steekproeven. Het wordt dan ook eenvoudiger om de onderrapportage te differentiëren naar verschillende delen van de populatie.

4. Social Media Text Profiling (SMTP)

SMTP bestaat uit tekstanalyse (textmining) van social media berichten waarmee geautomatiseerd bepaalde kwalificaties aan de berichten kunnen worden toegekend, bijvoorbeeld of er sprake is van bedreiging. SMTP is uiteraard alleen geschikt voor de analyse en schatting van online delicten die voldoende tekst produceren, dus over het algemeen online delicten met een duidelijke sociale of interactieve component, zoals bedreiging, afpersing, mogelijk het verspreiden van seksueel getint beeldmateriaal, en minder voor bijvoorbeeld computervredebreuk. Overigens bestaan er ook technieken voor de analyse van beeldmateriaal. Die zijn verder niet in dit onderzoek betrokken.

Conclusies over (potentiële) opbrengst

Met SMTP-technieken kan de rol van diverse betrokkenen worden bepaald, bijvoorbeeld dader, slachtoffer, handlanger, toeschouwer en kunnen de auteurs van berichten worden geïdentificeerd. In principe maken de resultaten van deze analyses het mogelijk om de aantallen daders en slachtoffers van bijvoorbeeld de bedreiging te tellen en/ of te schatten. Aan de verschillende betrokkenen kunnen diverse kenmerken worden toegekend, zoals de gebruikelijke achtergrondkenmerken als leeftijd, geslacht en opleiding, maar ook moeilijker te achterhalen attributen als persoonlijkheidskenmerken en politieke oriëntatie. Over de vraag of cybercriminaliteit in of vanuit het buitenland is te traceren zijn we in de geraadpleegde literatuur geen uitspraken tegengekomen. Er zijn geen redenen om te veronderstellen dat jeugdigen voor de methode een bijzondere analytische uitdaging betekenen. Mogelijk dat de analyses vaker moeten worden uitgevoerd vanwege een snelle evolutie van specifiek taalgebruik onder jongeren op social media.

Social Media analyse biedt de meest rechtstreekse manier om online delicten te analyseren. De analyses zijn te typeren als een vorm van ‘digitaal sporenonderzoek’ van online delicten. Andere methoden stellen vragen aan mogelijke daders of slachtoffers, of maken gebruik van gegevens over aangiften of meldingen bij de politie. In alle gevallen zijn er meer schakels tussen het verschijnsel cybercriminaliteit en onderzoeksgegeven.
In de tweede plaats belooft de analyse van social media data een betrekkelijk goedkope en daardoor ook frequent toe te passen alternatief of aanvulling te zijn voor de gebruikelijke methoden. In een minimumvariant kan een onderzoek worden uitgevoerd door een team van een senior-onderzoeker en twee junior-onderzoekers, ieder voorzien van een krachtige PC.

De aanpak is vooralsnog echter vooral een belofte. Op grond van ons onderzoek concluderen we dat er in deze hoek nog geen methode beschikbaar is die op dit moment ingezet kan worden voor het schatten van de omvang van een online delict. Onderdelen van de benodigde aanpak zijn in verre mate ontwikkeld en worden wel al operationeel gebruikt. Er bestaan echter nog geen voorbeelden

van onderzoek waarbij de verschillende onderdelen geïntegreerd zijn ingezet om een telling of schatting van een populatie te maken. Een cruciaal onderdeel, '(open class) authorship attribution', is volgens de literatuur nog onvoldoende ontwikkeld om met goed resultaat realistische analyses van auteurschap van onlinecommunicatie te doen.
Een andere beperking is dat er geen data openbaar beschikbaar zijn om met SMTP landelijke schattingen te maken van online criminaliteit. De data van social media zijn in principe niet openbaar en niet voor analyse beschikbaar. Wel kan de Nationale Politie toegang tot de data van Twitter verkrijgen.

Aanbevelingen
De aanpak zou nog een keer door een expert in SMTP in samenspraak met een expert in schattingsmethoden moeten worden beoordeeld op haalbaarheid. De afzonderlijke componenten zouden vervolgens tot één betrouwbare schattingsmethode moeten worden samengesmeed.

Met de beperkte beschikbare data zou dan een deel van de markt in kaart zijn te brengen. De Nationale Politie beschikt over Twittergegevens waarmee deze exercitie is uit te voeren. Hoewel een schatting met deze gegevens niet representatief is voor de gehele populatie, zouden herhaalde schattingen gedurende een reeks van jaren met aanvullende analyses opgevat kunnen worden als een indicatie van een landelijke trend.
Een mogelijkheid om een vollediger landelijk beeld te krijgen is een geheel ontwikkelde schattingsmethode ter beschikking te stellen aan providers en hen ertoe te bewegen de resultaten periodiek te rapporteren.

5. Vangst-hervangst schattingen en het 'mijnen' van politiedata

Vangst-hervangst methoden bieden een effectieve, efficiënte en beproefde methode om het aantal daders of slachtoffers van een delict te schatten en zijn een aantrekkelijk alternatief voor enquêtes. Het betreft een groep statistische methoden waarmee op basis van het aantal malen dat iemand voorkomt in een registratie, een schatting kan worden gemaakt van het aantal personen dat tot dezelfde groep behoort, maar niet is geregistreerd. Vaak worden als bron voor de gegevens politieregistraties of registraties van andere handhavingsinstanties gebruikt. Eerdere voorbeelden betreffen schattingen van het rijden onder invloed, vuurwapenbezit, illegaal verblijf in Nederland en huiselijk geweld.

Conclusies over (potentiële) opbrengst
Met behulp van deze methoden kan informatie worden verkregen over aantallen daders, daderkenmerken en kenmerken van het delict, zoals de directe financiële schade. In principe kan voor alle gegevens die zijn geregistreerd het onbekende deel ('dark number') worden bijgeschat. Een beperking is dat er geen schattingen kunnen worden gemaakt van verschijnselen of kenmerken die niet op een gestandaardiseerde wijze worden geregistreerd. Te denken valt aan motieven van daders of modus operandi, daders of slachtoffers in het buitenland. Ook is het niet mogelijk om het aantal incidenten of delicten te schatten.

Online delicten zijn een betrekkelijk nieuwe vorm van criminaliteit. De politieregistraties zijn er nog niet voldoende op ingericht om deze vorm van criminaliteit adequaat vast te leggen. In dit onderzoek

is nagegaan of de politieregistratie voldoende gegevens over de drie geselecteerde delicten bevat om er vangst-hervangst schattingen mee te maken.
Op basis van textmining van politiedata is een classifier ontwikkeld waarmee gegevens over online delicten geautomatiseerd uit de politieregistratie zijn te lichten. De gebruikte dataset bestaat uit aangiften uit de Basisvoorziening Handhaving (BVH) van de Nederlandse Politie. De aangiften hebben betrekking op de jaren 2013-2015. Ze zijn verkregen door een extractie uit de volledige BVH-registratie van die jaren met een zeer brede query bestaande uit een groot aantal begrippen gerelateerd aan online verschijnselen en activiteiten.
Een steekproef uit de data-extractie is geannoteerd. Op basis van textmining van de geannoteerde data zijn classifiers ontwikkeld. Met de beste classifiers voor elk van de drie geselecteerde online delicten, zijn alle beschikbare aangiften geclassificeerd, d.w.z. er is bepaald of er sprake was van een van de drie delicten. Vervolgens is per geregistreerde verdachte, per delict, per jaar een telling gemaakt van het aantal malen dat proces-verbaal tegen de verdachte is opgemaakt.
De telling laat zien dat voor twee van de drie geselecteerde delicten, online bedreiging en het online verspreiden van seksueel getint beeldmateriaal, voldoende 'vangsten' en 'hervangsten' beschikbaar zijn om er omvangschattingen voor de geselecteerde jaren mee te maken.

Aanbevelingen
De uitkomst van de textmining van BVH biedt de mogelijkheid om voor de twee delicten een onderzoek uit te voeren met als doel het maken van een eerste schatting met vangst-hervangst. De indeling van de geregistreerde delicten is echter nog zeer globaal. Er is geen onderscheid gemaakt naar ernst of verschillende verschijningsvormen van de delicten. Indien ervoor wordt gekozen om vangst-hervangst schattingen te maken, is het zaak eerst te onderzoeken of een nadere indeling van het betreffende delict zinvol is en of deze ook in de registratie is aan te brengen door middel van annotatie. Het is verstandig om daarbij een grotere steekproef te annoteren dan binnen het bestek van het onderhavige onderzoek mogelijk bleek.
Een tweede belangrijke conclusie van deze exercitie is dat textmining een interessante methode blijkt te zijn om efficiënt en effectief niet gestandaardiseerde gegevens uit de BVH te ontsluiten en geschikt te maken voor het vangst-hervangstschattingen.

6. Tot slot: de belangrijkste conclusies en aanbevelingen

Ons vooronderzoek heeft geen nieuwe methode opgeleverd die in de startblokken staat om een schatting van online delicten van jeugdigen te geven. Voor de twee nieuwere methoden, NSUM en SMTP, staan nog belangrijke vragen open. De twee meer vertrouwde methoden, vangst-hervangst en randomized response, kunnen, indien gewenst, wel ingezet worden. We geven tot slot nog een kort overzicht van de belangrijkste conclusies en aanbevelingen.

Vangst-hervangst
Uit het textmining onderzoek blijkt dat de politieregistratie voor twee van de drie geselecteerde delicten, online bedreiging en het online verspreiden van seksueel getint beeldmateriaal, voldoende zaken bevat om vangst-hervangst schattingen te maken. De gemaakte indeling naar drie online delicten is echter nog zeer globaal en onderscheidt niet naar ernst of verschillende verschijningsvormen. Het is aan te bevelen om eerst te bepalen of een zinvolle nadere indeling van

de betreffende delicten is te maken. Vervolgens dient een voldoende ruime steekproef van zaken aan de hand van deze indeling te worden geannoteerd.

Randomized response

Randomized response biedt in vergelijking met directe bevraging extra bescherming van anonimiteit voor respondenten bij onderwerpen die gevoelig liggen en die ze mogelijk liever verborgen houden, tegen de kosten van een (mogelijk aanzienlijk) grotere steekproef. Beide methoden kunnen vergelijkbare vragen beantwoorden.

Het is niet duidelijk of er voldoende aanleiding is om de extra kosten voor grotere steekproeven met randomized response te maken. Als eerste is de vraag aan de orde of randomized response in vergelijking met de directe vragen in de MZJ een significante en interessante verbetering van de rapportage oplevert. Een eerste, kostenbesparende indicatie hiervoor is te verkrijgen door de vergelijking op te nemen in een internetpanel.

NSUM

NSUM kan waarschijnlijk betrekkelijk eenvoudig schattingen leveren van online criminaliteit, zonder ingrijpende of kostbare aanpassingen van bestaand onderzoek zoals de MZJ. De methode lijkt vooral geschikt voor een omvangschatting van delicten met een sociale component, i.c. online bedreiging en het online verspreiden van seksueel getint beeldmateriaal. Met de methode kan het aantal daders en mogelijk nog een aantal eenvoudig vast te stellen kenmerken van daders en delicten worden geschat. NSUM is daarom geen vervanging van andere methoden, maar kan mogelijk dienen als onderdeel van een triangulatie.

Het lijkt ons verstandig om de prestaties en een aantal van de meer interessante modaliteiten van de methode eerst uit te proberen in een vergelijkend onderzoek. Zo'n onderzoek moet inzicht geven in de vraag of NSUM significant betere schattingen oplevert van geselecteerde online delicten van jeugdigen en wat daarvoor de beste opzet zou zijn.

Op kortere termijn is met betrekkelijk beperkte middelen met een simulatiestudie al meer zicht te krijgen op de mogelijkheden van de methode en van de validiteit en betrouwbaarheid van de schattingen die ermee zijn te maken.

SMTP

Tot slot, SMTP. Wij blijven gecharmeerd van de benadering, maar een echte schattingsmethode mag het nog niet heten. De aanpak zou in de eerste plaats nog een keer moeten worden beoordeeld en uitgeprobeerd op de mogelijkheid er betrouwbare tellingen en schattingen mee te maken. Databestanden met landelijke dekking ontbreken. Dat betekent dat een SMTP-schatting alleen een beperkt deel van online delicten in kaart kan brengen. Bij een periodieke herhaling is dit met aanvullende analyses mogelijk te interpreteren als een indicator van trends.