In- en doorstroom van online criminaliteit in de strafrechtketen

Stijn Ruiter
Merel van Leuken
Teun van Ruitenburg
Jim Schiks
Rutger Leukfeldt

Amsterdam, 2023

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

Samenvatting

Onze huidige samenleving is in sterke mate gedigitaliseerd. Met de digitalisering van de maatschappij is ook criminaliteit gedigitaliseerd en daarmee is het werkaanbod van politie en justitie veranderd. De strafrechtketen krijgt meer en meer te maken met delicten met een digitale component, ook wel online criminaliteit genoemd. Enerzijds is er sprake van nieuwe delicten, bijvoorbeeld het hacken van een database met persoonsgegevens of het platleggen van websites of netwerken. Dit soort delicten valt onder de noemer cybercrime. Anderzijds zijn er traditionele vormen van criminaliteit waarbij ICT een steeds belangrijkere rol speelt bij de realisatie daarvan. Voorbeelden zijn het plegen van fraude via internet en stalking. Dergelijke delicten vallen onder de noemer gedigitaliseerde criminaliteit.

Uit slachtofferenquêtes blijkt dat tegenwoordig meer burgers slachtoffer worden van hacken, online oplichting en online fraude dan van fietsendiefstal. Burgers en bedrijven worden daarnaast van nog veel meer vormen van online criminaliteit slachtoffer: van malware of ransomware tot phishing, cyberstalking en cyberbedreiging. Hoewel het inmiddels duidelijk is dat online criminaliteit een groeiend probleem is en dat er veel slachtoffers worden gemaakt, lijkt de in- en doorstroom van online criminaliteit in de strafrechtketen achter te blijven bij de ontwikkeling van het slachtofferschap van online criminaliteit zoals gerapporteerd in de Veiligheidsmonitor van het Centraal Bureau voor de Statistiek. Terwijl er blijkbaar veel slachtoffers worden gemaakt, is het aantal veroordelingen van daders van online criminaliteit gering.

Eerder onderzoek laat zien dat er in ieder geval drie oorzaken ten grondslag liggen aan het grote verschil in het aantal slachtoffers en het aantal veroordelingen: een lage aangiftebereidheid, de organisatie van politie en justitie die nog onvoldoende is ingericht om dergelijke zaken effectief op te pakken en de complexiteit van zaken. Naast deze oorzaken voor daadwerkelijk minder in- en doorstroom van online criminaliteit in de strafrechtketen, doet zich ook het probleem voor dat veel vormen van online criminaliteit - met name vormen van gedigitaliseerde criminaliteit - niet als zodanig herkenbaar zijn in de registraties van politie en justitie. Daarmee is mogelijk niet alleen de feitelijke in- en doorstroom gering, maar is er daarnaast ook beperkt zicht op de in- en doorstroom die er wel degelijk is.

Onderhavig onderzoek is erop gericht meer zicht te bieden op de in- en doorstroom van online criminaliteit in de strafrechtketen. Naast inzicht in de actuele in- en doorstroom biedt het onderzoek ook inzicht in mogelijke knelpunten binnen de strafrechtketen, *good practices* en verbetermogelijkheden.

Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Zijn er volgens de literatuur vormen van online criminaliteit waarvan verdachten niet of nauwelijks de strafrechtketen instromen? Zo ja, welke? Welke verklaringen worden er in de literatuur gegeven voor die lage instroom?
2. Wat zijn de meest recente cijfers over 2018-2020 met betrekking tot de instroom en doorstroom van online criminaliteit in de strafrechtketen?
3. Welke knelpunten kunnen geïdentificeerd worden binnen de in- en doorstroom van online criminaliteit in de strafrechtketen?
4. In hoeverre hebben andere landen ook te maken met de onder vraag 3 geconstateerde knelpunten? Welke ervaringen zijn er in andere landen met het oplossen van deze knelpunten?
5. Welke verbeteringen kunnen per schakel van de strafrechtketen worden doorgevoerd om de strafrechtpleging bij online criminaliteit te bevorderen?

Onderzoeksmethoden

Om de onderzoeksvragen te beantwoorden hebben we gebruik gemaakt van verschillende onderzoeksmethoden.

We deden een internationaal literatuuronderzoek om inzicht te krijgen in welke vormen van online criminaliteit niet of nauwelijks instromen in de strafrechtketen, welke verklaringen daarvoor zijn, welke knelpunten binnen de strafrechtketen kunnen zorgen voor beperkte doorstroom van zaken en wat mogelijke verbeterpunten zijn binnen de diverse schakels van de strafrechtketen om de doorstroom van zaken juist te bevorderen.

Voor de kwantitatieve analyse van de in- en doorstroom van online criminaliteit in de strafrechtketen namen we BVH-registraties van de politie als startpunt. Omdat veel vormen van online criminaliteit niet als zodanig herkenbaar worden geregistreerd in de systemen, ontwikkelden we *predictive textmining* modellen. Dergelijke modellen kunnen op basis van relevante tekstkenmerken documenten met grote hoeveelheden tekst automatisch classificeren. We maakten daarbij gebruik van *supervised machine learning*. Bij deze techniek wordt een model getraind aan de hand van voorbeelddocumenten waarvan vooraf handmatig is vastgesteld welk label zij dienen te hebben. Na de training wordt verondersteld dat het model nieuwe documenten zelf van het juiste label kan voorzien. We ontwikkelden de modellen op basis van een selectieve steekproef (n=7.500) waarin relatief veel registraties van online criminaliteit voorkwamen en pasten de modellen vervolgens toe op een grote willekeurige steekproef (n=300.000) van unieke BVH-registraties uit de jaren 2018-2020. Voor het vaststellen van de doorstroom in de strafrechtketen koppelden we de BVH-gegevens aan gegevens ontleend aan het systeem Betere Opsporing door Sturing op Zaken (BOSZ). Voor het

vaststellen van de doorstroom richting OM en rechtspraak hebben we vervolgens de gegevens over de naar het OM ingezonden verdachten gekoppeld aan gegevens ontleend aan het Geïntegreerd Processysteem Strafrecht (GPS). Om na te gaan in hoeverre de in- en doorstroom van online criminaliteit afwijkend is, herhaalden we dezelfde analyses voor drie andere vormen van criminaliteit (vermogenscriminaliteit, misdrijven tegen de lichamelijke integriteit en fraudedelicten).

Naast het literatuuronderzoek en de grootschalige kwantitatieve analyse van gegevens van politie en justitie zijn voor dit onderzoek allerlei gesprekken gevoerd. Het doel van de interviews met actoren binnen de verschillende schakels van de strafrechtketen was om zicht te krijgen op algemene knelpunten in de in- en doorstroom van online criminaliteit in de strafrechtketen. In totaal interviewden we 34 actoren binnen de strafrechtketen, waarvan 26 werkzaam waren bij de politie, 6 bij het OM en 2 bij de zittende magistratuur. Er is gesproken met medewerkers uit verschillende teams, waaronder basisteams (BT), de districtsrecherche (DR) en de Dienst Regionale Recherche (DRR) binnen de volgende 5 eenheden van de politie: Den Haag, Noord-Holland, Noord-Nederland, Midden-Nederland en Zeeland-West-Brabant. Binnen het OM zijn officieren van justitie die online criminaliteit in hun portefeuille hebben geïnterviewd. Hier zijn de parketten geselecteerd die samenwerken met de geselecteerde eenheden van de politie. Bij de zittende magistratuur zijn twee rechters bevraagd die zaken met een online component hebben behandeld.

Om zicht te krijgen op eventuele *good practices* in andere landen die ook in Nederland toepasbaar zouden kunnen zijn, interviewden we 5 internationale experts (uit het Verenigd Koninkrijk, de Verenigde Staten en Australië). Doel van deze interviews was om zicht te krijgen op de mate waarin andere landen ook te maken hebben met de knelpunten die we in de interviews met actoren binnen de strafrechtketen vernamen en welke ervaringen er in die landen zijn met het oplossen van deze knelpunten. De resultaten van de literatuurstudie, kwantitatieve analyses en interviews zijn ten slotte bediscussieerd met experts van binnen en buiten politie en justitie. De discussiebijeenkomsten zijn tevens gebruikt om te inventariseren welke mogelijke oplossingen er zijn om de geïdentificeerde knelpunten te verbeteren. In totaal deden 5 experts aan de discussiesessies mee.

Wel slachtofferschap, geen instroom

Eerder onderzoek laat zien dat de aangiftebereidheid onder slachtoffers van online criminaliteit over het algemeen lager is dan bij slachtoffers van traditionele delicten. Uit Nederlandse studies blijkt dat ongeveer 13% van de slachtoffers van online criminaliteit melding doet bij de politie. De bereidheid van slachtoffers om aangifte te doen bij de politie verschilt voor verschillende vormen van online criminaliteit. Bij delicten waar IT niet alleen het middel maar ook het doelwit is (cybercrimes) lijkt de aangiftebereidheid lager te liggen

dan bij delicten waarbij IT alleen als hulpmiddel wordt gebruikt (gedigitaliseerde criminaliteit). Uit eerdere studies blijkt dat het type online criminaliteit een belangrijke voorspeller is voor de aangiftebereidheid van online criminaliteit. Verder is de (waargenomen) ernst van een delict een belangrijke voorspeller: hoe ernstiger het delict, hoe eerder aangifte wordt gedaan.

Er worden in de literatuur verschillende verklaringen genoemd waarom slachtoffers van online criminaliteit geen aangifte doen. Zo weten individuen en bedrijven niet altijd dat ze slachtoffer zijn of zien slachtoffers online incidenten zoals malware-infecties niet als criminaliteit. In de gevallen waarbij slachtoffers wel op de hoogte zijn van hun slachtofferschap, kunnen verschillende factoren ertoe leiden dat ze toch geen aangifte doen. Een veelgenoemde verklaring is dat individuen de ernst en impact van online delicten als laag ervaren en daardoor minder snel geneigd zijn om aangifte te doen. In andere gevallen is er geen of weinig (financiële) schade of is de schade al vergoed door bijvoorbeeld verzekeringsmaatschappijen of financiële instellingen. Verder kan schaamte een rol spelen bij het niet melden van slachtofferschap. Ten slotte kan spelen dat slachtoffers een gebrek aan vertrouwen hebben in de politie om daders van online criminaliteit op te sporen en aan te houden.

In- en doorstroom in cijfers

De in- en doorstroom van online criminaliteit in de strafrechtketen is voor de jaren 2018-2020 geanalyseerd. Daartoe zijn BVH-registraties van de politie uit die periode als startpunt genomen. In het BVH-systeem registreert de politie incidenten, meldingen en aangiften en de aan de incidenten gekoppelde acties zoals processen-verbaal van verhoor van getuigen of verdachten. Omdat de verschillende vormen van online criminaliteit niet systematisch in de BVH-registraties kunnen worden geïdentificeerd aan de hand van bijvoorbeeld unieke maatschappelijke klassen, zijn *predictive textmining* modellen ontwikkeld die gebruikmaken van alle bij een BVH-registratie behorende registraties van *bevindingen*, *toelichtingen*, *verklaringen* en *MO-teksten.* Er zijn afzonderlijke modellen ontwikkeld om negen verschillende typen online criminaliteit te onderscheiden: vier vormen van cybercrime (hacking, malware, ransomware en DDoS-aanval) en vijf vormen van gedigitaliseerde criminaliteit (online bedreiging, online stalking, online smaad/laster/belediging, online oplichting en *money muling*), waarbij we online oplichting nog uitsplitsten naar phishing, online identiteitsfraude, online aan- en verkoopfraude, VIN-fraude, helpdeskfraude en overige online oplichting. De *predictive textmining* modellen hadden niet voor alle vormen van online criminaliteit een voldoende goede *performance* om ermee de afzonderlijke vormen van online criminaliteit in BVH-registraties te kunnen identificeren. Voor de overkoepelende labels cybercrime en gedigitaliseerde criminaliteit als ook voor de afzonderlijke labels hacking, online oplichting, phishing, online identiteitsfraude,

online aan- en verkoopfraude, VIN-fraude en helpdeskfraude was de *performance* goed en voor die vormen konden daarmee beschrijvende analyses van de in- en doorstroom in de strafrechtketen worden gepresenteerd.

Door de modellen met een goede *performance* toe te passen op een grote steekproef (n=300.000) van BVH-registraties kon de in- en doorstroom van online criminaliteit in de periode 2018-2020 worden bestudeerd. BVH-registraties met een aangifte vormen een duidelijk startpunt van de strafrechtketen en BVH-registraties die geclassificeerd zijn als online criminaliteit en waarbij tenminste 1 aangifte is geregistreerd markeren dan ook wat we in kwantitatieve analyse de *instroom* van online criminaliteit in de strafrechtketen hebben genoemd.

De belangrijkste bevinding uit de kwantitatieve analyse van in- en doorstroom van online criminaliteit in de strafrechtketen is gelegen in de lage aantallen. We startten de analyse met een relatief grote steekproef van BVH-registraties (n=300.000) om vervolgens vast te stellen dat de meeste vormen van online criminaliteit in minder dan 1% (met maximum van 4% voor alle gedigitaliseerde criminaliteit tezamen) van de registraties voorkwam. Van de hoge prevalentie die wordt vastgesteld in slachtofferenquêtes zien we in BVH-registraties dus weinig terug. Vervolgens bleek in ongeveer 25% van de registraties geen sprake te zijn van een aangifte en van alle registraties met een aangifte werd maar in ongeveer 10% van de gevallen ook een verdachte gekoppeld. De belangrijkste conclusie moet dan ook luiden: we vinden zelfs met de toepassing van geavanceerde *predictive textmining* modellen maar weinig registraties van online criminaliteit in de strafrechtketen. De instroom in de vorm van aangiften is al niet groot, maar omdat er maar in ongeveer 10% van de gevallen een verdachte wordt gekoppeld, is de doorstroom nog veel geringer.

Verder laten de resultaten van de grootschalige kwantitatieve analyses zien dat BVH-registraties die als gedigitaliseerde criminaliteit zijn geclassificeerd aanzienlijk meer voorkomen dan registraties van cybercrime. De 25% van de BVH-registraties die geclassificeerd zijn als cybercrime of gedigitaliseerde criminaliteit waarbij geen sprake was van een aangifte wijst erop dat er in het BVH-systeem ook best vaak mutaties over online criminaliteit worden gemaakt zonder dat er sprake is van een aangifte. Wanneer we deze cijfers echter vergelijken met die voor andere vormen van criminaliteit, dan valt op dat dit niet uniek is voor online criminaliteit. Bij misdrijven tegen de lichamelijke integriteit (32%) en fraudedelicten (51%) liggen de percentages zelfs nog aanzienlijk hoger, terwijl het percentage bij vermogensdelicten (11%) juist lager is. Het maken van een BVH-mutatie zonder een aangifte op te nemen is dus niet uniek voor online criminaliteit.

Het lage percentage BVH-registraties van online criminaliteit met een aangifte waarbij ook tenminste 1 verdachte staat geregistreerd (8% voor cybercrime en 10% voor gedigitaliseerde criminaliteit) blijkt flink te variëren tussen afzonderlijke vormen van online criminaliteit, van slechts 2% bij online aan- en

verkoopfraude tot 18% bij helpdeskfraude. Daarbij blijkt bovendien dat bij de vormen van online criminaliteit die relatief veel voorkomen juist relatief weinig verdachten worden geregistreerd.

88% van de verdachten van cybercrime en 85% van de verdachten van gedigitaliseerde criminaliteit was meerderjarig, al valt op dat het aandeel minderjarige verdachten wat hoger is bij helpdeskfraude (21%) en juist wat lager bij VIN-fraude (8%), online identiteitsfraude (8%) en online oplichting (9%).

Voor een aanzienlijk deel van de meerderjarige verdachten van online criminaliteit zien we een overige of onbekende afdoening geregistreerd staan bij politie of OM (samen goed voor 43%), terwijl dit bij minderjarige verdachten ook maar in mindere mate voorkomt (33%). Het aandeel van de verdachten van online criminaliteit die helemaal doorstromen naar de rechtbank verschilt weinig tussen meerderjarige en minderjarige verdachten, en ligt rond eenderde. Minderjarige verdachten krijgen vaker een afdoening bij de politie (6%) dan meerderjarigen verdachten (1%).

Om de in- en doorstroom van online criminaliteit in perspectief te plaatsen, zijn dezelfde analyses gedaan voor drie andere vormen van criminaliteit, te weten *vermogenscriminaliteit*, *misdrijven gericht tegen de lichamelijke integriteit*, en *fraudedelicten*. We zien aanzienlijk meer BVH-registraties van vermogenscriminaliteit dan van online criminaliteit. De aantallen voor misdrijven gericht tegen de lichamelijke integriteit liggen juist net iets lager en voor fraudedelicten zien we nog veel minder registraties. Het percentage BVH-registraties waarbij ook tenminste 1 aangifte was geregistreerd lag hoger bij vermogenscriminaliteit dan bij online criminaliteit, maar bij de andere vormen van criminaliteit lag het juist lager. Bij vermogenscriminaliteit zien we ongeveer even vaak een verdachte geregistreerd staan (in 12% van de gevallen) als bij online criminaliteit (10%). Bij fraudedelicten ligt het percentage BVH-registraties met aangifte waarbij tenminste 1 verdachte is geregistreerd aanzienlijk hoger (31%), terwijl dit bij misdrijven gericht tegen de lichamelijke integriteit nog veel hoger (59%) ligt. De ophelderingspercentages liggen bij deze laatste twee vormen van criminaliteit dus aanzienlijk hoger dan bij online criminaliteit en vermogenscriminaliteit. Voor misdrijven tegen de lichamelijke integriteit is dit niet zo verwonderlijk, aangezien dader en slachtoffer vrijwel altijd direct met elkaar in contact zullen zijn geweest en er dan ook vaak sprake is van daderindicatie, terwijl bij online criminaliteit en vermogenscriminaliteit de verdachte vaak niet direct in beeld zal zijn. Dit verklaart echter niet het verschil in ophelderingspercentages bij online en offline fraudedelicten.

Zodra er een verdachte in beeld is, zien we ook bij vermogenscriminaliteit en misdrijven tegen de lichamelijke integriteit dat minderjarige verdachten vaker een afdoening bij de politie krijgen dan meerderjarige verdachten. Verder valt op dat een hoog percentage meerderjarige verdachten van vermogenscriminaliteit

helemaal doorstroomt tot de rechtbank (55%). Ook bij misdrijven tegen de lichamelijke integriteit (46%) en fraudedelicten (43%) ligt dit percentage aanzienlijk hoger dan bij online criminaliteit (32%).

Knelpunten volgens de literatuur en volgens actoren binnen de strafrechtketen

Intake

Uit de literatuur blijkt dat de politie niet altijd een aangifte opneemt wanneer slachtoffers van online criminaliteit contact opnemen met de politie. Dat kan komen doordat intakemedewerkers denken dat het niet om een strafbaar feit gaat (bijvoorbeeld in hacking zaken), dat het om een civiele zaak gaat (bijvoorbeeld bij online fraude) of meer algemeen dat intakemedewerkers de ernst van het slachtofferschap als laag inschatten. Indien er wel een aangifte wordt opgenomen, dan lijkt het succesvol opnemen van een aangifte afhankelijk te zijn van het begrip en de kennis van de intakemedewerker die de aangifte van online criminaliteit opneemt. Deze kennis is echter niet altijd (voldoende) aanwezig bij intakemedewerkers.

Respondenten geven aan dat ze een gebrek aan kennis van online criminaliteit zien onder intakemedewerkers, terwijl juist een kwalitatief hoogstaande aangifte voor een succesvolle doorstroom in de strafrechtketen zorgt. Een knelpunt is verder dat de aangifte ook afhankelijk is van (de kennis van) de aangever. Het ‘verhaal’ van de aangever is lang niet altijd helder. Burgers weten zelf ook niet altijd precies wat er is gebeurd. Des te belangrijker is het voor intakemedewerkers om de juiste vragen te stellen. Het geautomatiseerde aangifteproces via de website van de politie maakt het mogelijk om beter door te vragen.

Zowel de experts die deelnamen aan de discussiesessies als de internationale respondenten die geïnterviewd zijn herkennen het beeld dat naar voren kwam uit de literatuur en interviews. Tijdens de expertsessies werd meermaals gewezen op de belangrijke rol die intakemedewerkers spelen bij het leggen van een goede basis voor verder opsporingsonderzoek. Zonder de juiste informatie is de kans op vroegtijdig uitval volgens de experts groter.

Casescreening

Er is relatief weinig onderzoek dat zich richt op de casescreening van zaken online criminaliteit door de politie. Uit het onderzoek dat wel is gedaan ontstaat het beeld dat online criminaliteit zaken minder snel worden opgepakt dan traditionele zaken. Verklaringen hiervoor zijn dat de afhandeling van dergelijke zaken veel tijd kost, een gebrek aan capaciteit, het internationale karakter van online criminaliteit en de kwaliteit van de opgenomen aangiften.

Uit de interviews komen verschillende redenen naar voren waarom zaken van online criminaliteit binnen het screeningsproces uitvallen. De belangrijkste reden die door respondenten wordt genoemd is het gebrek aan

opsporingsindicatie en meer concreet het ontbreken van een verdachte. Hoewel dit geen uniek probleem is, speelt dit volgens respondenten in het bijzonder bij online criminaliteit, omdat daders zichzelf en de illegaal verkregen inkomsten makkelijker en effectiever kunnen afschermen. Daarbij blijkt het voor online criminaliteit lastiger dan voor traditionele criminaliteit in te schatten of een zaak voldoende opsporingsindicatie bevat. Voor het al dan niet oppakken van een zaak speelt ook de financiële schade een rol. Is sprake van een 'gering' schadebedrag dan wordt een zaak niet of minder snel opgepakt.

Opsporing

Ook wanneer wordt besloten om een zaak op te pakken, kunnen er verschillende redenen zijn waarom een zaak tijdens de opsporing alsnog uitstroomt. Uit de literatuur komen vier factoren naar voren die de opsporing van online criminaliteit bemoeilijken. Ten eerste wordt het gebrek aan prioriteit binnen politieorganisaties genoemd, wat onder meer versterkt wordt door de complexiteit van deze opsporingszaken en het beperkte bewustzijn van de risico's van online criminaliteit. Ten tweede bestaat er te weinig kennis en vaardigheden onder politiemedewerkers om opsporingsonderzoeken inzake online criminaliteit (effectief) op te pakken. Ten derde komt uit de literatuur naar voren dat ook bij de opsporing te weinig capaciteit aanwezig is om online criminaliteit op te pakken, waarbij politiemedewerkers met specialistische kennis moeilijker binnen de politieorganisatie te behouden zijn. Tot slot geldt dat de complexiteit van online criminaliteit de opsporing van daders verder bemoeilijkt. Dit komt bijvoorbeeld door het internationale karakter van online criminaliteit en de vluchtigheid van digitale gegevens.

De knelpunten die in de literatuur worden benoemd, zijn op soortgelijke wijze teruggekomen tijdens de interviews en worden ook benoemd in de discussiesessie: een gebrek aan prioriteit, een gebrek aan kennis, een gebrek aan capaciteit en de complexiteit van online criminaliteitszaken. Voor wat betreft het gebrek aan prioriteit werd door respondenten vooral gesproken over de gepercipieerde lagere (sociale) impact van online criminaliteit, hoewel dit door een deel van de respondenten als onterecht wordt beschouwd. Algemeen gesteld lijken de werkprocessen van de politieorganisatie nog voornamelijk te zijn ingericht op traditionele vormen van criminaliteit. Heterdaadsituaties, bijvoorbeeld bij winkeldiefstallen, krijgen voorrang op online criminaliteit zaken. Tegelijkertijd dient te worden opgemerkt dat de afgelopen jaren een duidelijke kentering zichtbaar is, waarbij verschillende teams speciaal zijn ingericht op het opsporen van online criminaliteit. Volgens respondenten wordt online criminaliteit door collega's nog vaak (onterecht) als iets ingewikkelds gezien. Ondanks toegenomen prioriteit voor het aanpakken van online criminaliteit, geeft het overgrote deel van de respondenten aan dat zowel de basisteams, de districtsrecherches als de cybercrimeteams, om verschillende redenen, kampen met een capaciteitsgebrek.

Tijdens de interviews wordt ook genoemd dat de opsporing van online criminaliteit complex is en dat deze complexiteit een knelpunt kan vormen voor de goede doorstroom hiervan. Alle factoren die online criminaliteit complex (kunnen) maken en in de literatuurstudie werden genoemd, werden ook tijdens de interviews genoemd. Veruit het meest genoemd was het internationale karakter van online criminaliteit en de perceptie dat het verkrijgen en behouden van digitaal bewijs lastig is door de vluchtigheid van gegevens in de online wereld. Daarnaast benoemen respondenten dat de politie als gevolg van wet- en regelgeving vaak over onvoldoende opsporingsmogelijkheden beschikt om digitaal bewijs veilig te kunnen stellen. In aanvulling op de literatuur wijzen respondenten ook nog op het potentieel grote aantal slachtoffers dat met online criminaliteit gepaard gaat en de mogelijkheid dat slachtoffers vaak niet binnen dezelfde eenheid woonachtig zijn.

Tot slot is aan bod gekomen dat het internationale karakter van online criminaliteit en het feit dat er vaak veel verschillende slachtoffers in meerdere eenheden zijn een gebrek aan eigenaarschap in de hand kan werken. Wanneer niet duidelijk is aan welk opsporingsteam een zaak toebehoort, kan dit er toe leiden dat een zaak niet wordt opgepakt.

De internationale respondenten schetsen eenzelfde beeld als de Nederlandse respondenten. Alhoewel het per land verschillend is, lijkt de situatie in het VK, de VS en Australië zelfs nog complexer door de veelheid van lokale politieregio's en de organisatie van de politie op federaal en statelijk niveau. Respondenten geven bijvoorbeeld aan dat het voor casescreeners lastig kan zijn om te bepalen waar een zaak 'gedraaid' moet worden omdat in veel gevallen lokale politiediensten zijn die een zaak kunnen oppakken, maar dat er ook landelijk opererende teams zijn die zich richten op georganiseerde misdaad en/of fraude en cybercrimes inmiddels ook in hun takenpakket hebben. Als een zaak dan naar een 'verkeerd' team gaat, dan is de kans volgens respondenten groot dat die nooit wordt opgepakt.

OM en ZM

Er bestaat weinig onderzoek dat ingaat op de knelpunten in de doorstroom van zaken binnen het OM of de ZM. In 2012 werd door Leukfeldt *et al.* nog geconcludeerd dat gespecialiseerde officieren van justitie op het gebied van online criminaliteit weinig of geen online criminaliteitszaken krijgen. Verder leken in dat onderzoek rechters geen knelpunten te ervaren in de afhandeling van online criminaliteitszaken, hoewel ze wel meer tijd kosten om goed te kunnen doorgronden. Andere knelpunten omtrent de vervolging van online criminaliteit zijn hetzelfde als voor de opsporing, en hebben te maken met wet- en regelgeving, bewijsvoering en de complexiteit van online criminaliteitszaken.

Opvallend is dat alle respondenten aangeven dat het merendeel van de knelpunten bij de politie ligt en in mindere mate bij OM en ZM. Over het algemeen stellen de respondenten dat er bij OM en ZM minder

problemen zijn op het gebied van capaciteit als het gaat om de afhandeling van online criminaliteit. Ook is het duidelijk dat online criminaliteit prioriteit heeft. Dat wil overigens niet zeggen dat er – met name bij het OM – buiten de politie geen knelpunten benoemd zijn. Zo geven respondenten bijvoorbeeld aan dat ook bij het OM – en in mindere mate ook ZM – er sprake is van digitale koudwatervrees. Een punt dat enkele malen tijdens de interviews aan bod kwam en ook door experts tijdens de discussiesessies werd benoemd is dat er wel knelpunten zijn door de gehanteerde definities van online criminaliteit. Streefdoelen van het OM met betrekking tot online criminaliteit zouden met name betrekking hebben op cybercrime in enge zin. Vormen van gedigitaliseerde criminaliteit kunnen daardoor eerder buiten de boot vallen volgens respondenten en experts. Dit komt overeen met bevindingen uit de literatuur en heeft volgens respondenten deels te maken met de wijze waarop online criminaliteit (juridisch) gedefinieerd wordt. Tenslotte geven zowel respondenten als experts tijdens de discussiesessie aan dat zaken kunnen uitstromen omdat het OM in plaats van dagvaarden kiest voor een alternatieve afdoeningswijze zoals '*knock-and-talk*'- of 'stop'-gesprekken. Dergelijke interventies zijn volgens respondenten en experts niet terug te zien in de gebruikelijke statistieken.

Verbetermogelijkheden volgens de literatuur, actoren binnen de strafrechtketen en experts uit binnen- en buitenland

Geen instroom

In de literatuur worden enkele suggesties gedaan om de aangiftebereidheid onder slachtoffers van online criminaliteit te verhogen. Een eerste aanbeveling betreft het inzetten van publieke bewustwordingscampagnes waarin de noodzaak wordt benadrukt om online criminaliteit te melden bij de politie. Een andere suggestie is om uniforme en gedegen aangiftesystemen op te zetten, bijvoorbeeld in de vorm van online aangiftesystemen. Zo zouden online aangiftesystemen de aangiftebereidheid van gebruikers om aangifte te doen van online criminaliteit verhogen. In Australië is bijvoorbeeld een online aangiftesysteem ontwikkeld speciaal voor online criminaliteit. Ten slotte wordt in de literatuur geopperd om de opportuniteitskosten (tijd, moeite en financiële kosten) voor het doen van aangifte te verminderen en de waargenomen voordelen van het aangifteproces te verhogen.

Intake en case screening

Uit de interviews blijkt dat het aangifteproces een belangrijke stap is in het proces van in- en doorstroom van online criminaliteit. Om de eerdergenoemde knelpunten in de intake van aangiften online criminaliteit te kunnen verbeteren, wordt in de literatuur aanbevolen om training op maat te geven aan intake- en servicemedewerkers. Ook respondenten en experts gaven tijdens de discussiesessie aan dat het goed

opleiden van intake medewerkers en/of casescreeners van groot belang is om de kwaliteit van aangiften te verbeteren.

Een door respondenten veelgenoemde verbetering betreft het landelijke clusteren en screenen van aangiften. Centralisatie zou ervoor moeten zorgen dat meer aangiften relevante informatie over verdachten bevatten en daarmee de opsporingskansen worden vergroot. Daarnaast kan het volgens respondenten tevens de efficiëntie van het politiewerk vergroten en het mogelijk maken om trends te signaleren en op basis daarvan de prioriteit te bepalen (bijvoorbeeld welke aangiften als eerste moeten worden opgepakt). Daarbij benadrukken respondenten het belang van geautomatiseerde dataverrijking en -analyse, met name omdat online criminaliteit minder tot de verbeelding zou spreken.

We merken graag op dat in lijn met het centraal verzamelen en screenen van online criminaliteitszaken, meerdere respondenten wijzen op bestaande initiatieven zoals het LMIO, de ECTF en Operatie Centurion.

Buitenlandse respondenten geven aan dat in het VK, de VS en Australië op eenzelfde manier wordt gezocht om problemen met betrekking tot intake en case screening op te lossen. Het meest kunnen we leren van de situatie in het VK en Australië. In het VK is er sprake van een gecentraliseerde intake van fraudezaken. In Australië zijn er voor verschillende vormen van criminaliteit centrale meldpunten waar burgers en bedrijven aangifte kunnen doen, waarna de aangifte naar het juiste politieteam wordt gestuurd. Sinds enkele jaren is er ook een landelijk meldpunt voor online criminaliteit. Een belangrijke les die we volgens respondenten van beide initiatieven kunnen leren is dat de centrale afhandeling van aangiften zorgt voor een veel betere registratie van aangiften en dat daarmee het totale aantal aangiften simpelweg snel omhoog zal gaan. Dat zegt echter niets over de verdere doorloop binnen de strafrechtketen. Respondenten geven aan dat ook verderop in de keten (van opsporingsteams tot OM en ZM) de capaciteit moet worden vergroot omdat er anders wel meer aangiften zijn die binnenstromen, maar er bij toename van de instroom gebrek aan capaciteit ontstaat om zaken op te pakken. De respondenten uit het VK geven daarbij aan dat ze zien dat er relatief veel aangiften alsnog meteen uitstromen, maar dat de aangiften die gebundeld en verrijkt zijn met informatie over de verdachte(n) er wel voor zorgen dat de zaken die ze doorsturen naar teams vaker succesvol worden opgepakt.

Opsporing

In de literatuur worden met name suggesties gedaan om het proces van de opsporing van online criminaliteit te verbeteren die gericht zijn op het wegnemen van koudwatervrees. Zo zouden trainingen ervoor kunnen zorgen dat rechercheurs bewuster worden over de mogelijke ernst van deze vormen van criminaliteit en zien dat onderzoeken lang niet altijd complex zijn. Daarnaast wordt genoemd dat opsporingsteams kunnen worden versterkt met mensen van buiten de politie omdat sommige burgers over meer expertise beschikken

op het gebied van online criminaliteit dan traditionele politiemedewerkers. Ten slotte wijzen studies er op dat er meer (inter-)nationale samenwerking nodig is tussen opsporingsinstanties zodat kennis over online criminaliteit, forensische methodes en opsporingstechnieken kunnen worden gedeeld.

Een punt voor verbetering aangaande de fase van opsporing die door zowel respondenten bij de politie als het OM wordt genoemd, houdt in dat het recherchewerk niet eindeloos door hoeft te gaan. Respondenten merken op dat daders van online criminaliteit meerdere slachtoffers tegelijkertijd kunnen maken en dat het soms lijkt alsof er eindeloos veel aangiften aan elkaar kunnen worden gekoppeld. Er moet volgens sommige respondenten dan ook 'slimmer worden opgespoord'. Het is niet altijd nodig om ál het bewijsmateriaal te verzamelen. Er kunnen ook vaker kosten-baten-overwegingen worden gemaakt en worden bekeken wat de investering (in tijd en menskracht) op gaat leveren.

OM en ZM

Door het beperkte aantal studies omtrent de in- en doorstroom van online criminaliteit bij het OM en de ZM, ontbreken aanbevelingen omtrent deze fasen in de strafrechtketen. Sommige aanbevelingen die in de literatuur worden genoemd om de in- en doorstroom van online criminaliteit te verbeteren hebben betrekking op meerdere fasen in de strafrechtketen of zelfs de gehele strafrechtketen. Zo wordt aanbevolen om lange termijnplannen te maken om vaardigheden van medewerkers te verbeteren, moet de effectiviteit van bestaande trainingen worden verbeterd en wordt aanbevolen aan strafrechtketenorganisaties om actief samen te werken met andere relevante publieke en private organisaties, zoals banken, online marktplaatsen, helpdesks en creditcard organisaties.

Tijdens de interviews werden er niet veel knelpunten omtrent de vervolging van online criminaliteit genoemd. Datzelfde geldt dan ook voor de mogelijke verbeterpunten. Een punt dat respondenten noemen en dat door experts tijdens de discussiesessies werd aangedragen is het organiseren van geschikte cursussen voor zowel OM als ZM om de koudwatervrees weg te nemen. Over andere verbeterpunten die genoemd werden bestaat verdeeldheid. Zo oordelen enkele officieren dat er een portefeuille 'gedigitaliseerde criminaliteit' (brede zin) aan officieren zou moeten worden toegekend, terwijl momenteel alleen portefeuillehouders 'cybercrime' (enge zin) zijn aangesteld. Anderen geven juist aan dat elke officier met dergelijke zaken aan de slag zou moeten kunnen en hiermee ervaring op zou moeten doen. Met betrekking tot de rechtspraak wordt als verbeterpunt genoemd om zogenoemde 'gelabelde' zittingen te organiseren. Hiermee wordt gedoeld op zittingen waarop in principe alleen online criminaliteitszaken worden behandeld. Op die manier behandelen rechters die gespecialiseerd zijn op dit thema deze zaken. De interviews laten wel zien dat er verschillend wordt gedacht over het belang van een gespecialiseerde groep rechters op dit thema.

Conclusies

Hoewel online criminaliteit volgens onderzoek gebaseerd op slachtofferenquêtes tegenwoordig tot de grootste vorm van criminaliteit behoort, blijken de meeste vormen van online criminaliteit door de wijze waarop het in de strafrechtketen wordt geregistreerd vaak niet als zodanig herkenbaar. Het zou enorm helpen wanneer bij de registratie van criminaliteit een uitgebreidere en ook regelmatig geactualiseerde lijst specifieke delicttypen zou worden gehanteerd, waardoor de verschillende verschijningsvormen op systematische wijze in kaart kunnen worden gebracht. Dit verbetert het informatiebeeld, maakt een gerichtere aanpak van de knelpunten in de strafrechtketen mogelijk en voorkomt dat een volgende studie wederom complexe analyses moet uitvoeren in een poging om de in- en doorstroom in beeld te brengen.

Waar de prevalentie van online criminaliteit op basis van slachtofferenquêtes juist erg hoog wordt geschat, vallen in de kwantitatieve analyses van BVH-registraties met name de lage instroomcijfers op. Gedigitaliseerde criminaliteit komt ongeveer 4 keer vaker voor dan cybercrime, maar de meeste vormen van online criminaliteit komen in minder dan 1% (het maximum ligt op 4% voor alle gedigitaliseerde criminaliteit tezamen) van de BVH-registraties voor. Dit beeld past bij wat bekend is over de lagere aangiftebereidheid bij online criminaliteit in vergelijking met die bij traditionele criminaliteit: veel gevallen van online criminaliteit stromen dus simpelweg nooit de strafrechtketen in.

De geïnterviewde experts zien de grootste uitdagingen aan de voorkant van de strafrechtketen, bij de politie. Met name de intake van online criminaliteit zou te wensen overlaten omdat kennis en expertise ontbreken. Dit zou ertoe leiden dat bij online criminaliteit er niet altijd een aangifte wordt opgenomen en soms alleen een melding wordt geregistreerd, waarmee de grootste bron van instroom (aangiften door burgers en bedrijven) stokt. Enerzijds klopt dit beeld met onze bevindingen. We constateerden immers dat waar de prevalentie van online criminaliteit op basis van slachtofferenquêtes erg hoog wordt geschat, in onze kwantitatieve analyses van BVH-registraties juist de lage instroomcijfers opvallen. Er is dus een groot verschil tussen door burgers ervaren – en in slachtofferenquêtes gerapporteerd – slachtofferschap en door de politie geregistreerd slachtofferschap. Verder troffen we in de kwantitatieve analyses inderdaad BVH-registraties van online criminaliteit zonder aangifte aan. Dit betrof ongeveer een kwart van de registraties. Dit is echter niet uniek voor online criminaliteit, want bij andere vormen van criminaliteit zagen we zelfs nog hogere percentages BVH-registraties zonder aangifte. Het is om die reden aan te raden om in vervolgonderzoek te kijken naar de discrepantie tussen ervaren slachtofferschap door burgers en door de politie geregistreerd slachtofferschap. Verder is het van belang om voor verschillende vormen van criminaliteit een nadere analyse te maken van de situaties waarin de politie een melding registreert in plaats van een aangifte opneemt.

Als slachtoffers van online criminaliteit wel aangifte hebben gedaan, dan blijkt dat er in 90% van de gevallen geen verdachte wordt geïdentificeerd. Dit wijst op een laag ophelderingspercentage en in combinatie met de al zeer beperkte instroom leidt het ertoe dat maar weinig zaken doorstromen in de strafrechtketen. Het percentage BVH-registraties met een aangifte waarbij tenminste één verdachte wordt geïdentificeerd verschilt overigens weinig tussen cybercrime en gedigitaliseerde criminaliteit, al valt op dat de percentages registraties met verdachte(n) juist laag zijn bij die vormen van online criminaliteit die het meest geregistreerd worden. Blijkbaar lukt het bij die zaken die het grootste deel van het werkaanbod van de politie bepalen het minst goed om er verdachten aan te koppelen. Met name het lage percentage bij online aan- en verkoopfraude (2%) is opvallend, aangezien er bij die vorm toch vaak bankrekeninggegevens beschikbaar zouden moeten zijn.

Hoewel de respondenten verschillende redenen noemden waarom opsporing bij online criminaliteit lastig is en dat er koudwatervrees bestaat, zijn lage ophelderingspercentages niet uniek voor online criminaliteit. Ook bij vermogenscriminaliteit zien we lage percentages (bij 12% van de BVH-registraties met een aangifte zagen we ook tenminste 1 verdachte geregistreerd staan), terwijl deze juist aanzienlijk hoger liggen bij fraudedelicten (31%) en al helemaal bij misdrijven tegen de lichamelijke integriteit (59%). Het verschil met misdrijven tegen de lichamelijke integriteit is wellicht niet zo verwonderlijk, omdat in die gevallen er vaak sprake zal zijn geweest van direct contact tussen dader en slachtoffer, waardoor er daderindicatie zal zijn. Het grote verschil tussen offline en online fraudedelicten is echter niet op deze wijze te verklaren. Hoewel we in deze studie niet kunnen uitsluiten dat de waargenomen verschillen samenhangen met verschillen in opsporingsinzet, komt uit de interviews naar voren dat de aanwezigheid van dader- of opsporingsindicatie een grote rol speelt bij de keuze om zaken op te pakken. Respondenten gaven aan dat dit bij online criminaliteit vaker ontbreekt waardoor zaken al sneuvelen bij de casescreening of verder niet succesvol worden opgepakt. Het ontbreken van dader- of opsporingsindicatie is echter niet uniek voor online criminaliteit, want dit speelt ook vaak bij vermogensdelicten.

Hoewel onder de respondenten consensus lijkt te bestaan dat de grootste uitdagingen in de in- en doorstroom van online criminaliteit binnen de strafrechtketen liggen binnen de politie, laten de kwantitatieve analyses zien dat er voor een aanzienlijk deel van de naar het OM ingestuurde verdachten sepots worden geregistreerd. Dat beeld zien we overigens ook voor de drie andere typen delicten waarmee we online criminaliteit vergeleken hebben. De redenen voor de sepots hebben we niet onderzocht, maar het beeld is dus niet uniek voor online criminaliteit. Daarmee lijkt het voor het verbeteren van de in- en doorstroom van online criminaliteit binnen de strafrechtketen inderdaad verstandig om vooral de aandacht te richten op de knelpunten en uitdagingen binnen de politie.

Het NSCR is onderdeel van de institutenorganisatie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)

Bezoekadres:
De Boelelaan 1077
1081 HV Amsterdam

Postadres:
Postbus 71304
1008 BH Amsterdam

T 020 598 5239
E nscr@nscr.nl
W www.nscr.nl

nscr

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving