Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

**Directoraat-Generaal**
**Straffen en Beschermen**
Directie Beschermen,
Aanpakken en Voorkomen
Slachtofferbeleid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

**Ons kenmerk**
2492849

*Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.*

Datum 7 februari 2019
Onderwerp Beleidsreactie WODC-onderzoek cybercrimeBeleidsreactie WODC-onderzoek cybercrime

In een sterke rechtsstaat ervaren slachtoffers genoegdoening door straffen, worden zij beschermd als dat nodig is en worden zij ondersteund bij het herstel van hun leed, zodat zij zo veel mogelijk zelf weer verder kunnen.[1] Dit geldt ook voor slachtoffers van online criminaliteit. Onder de noemer 'online criminaliteit' vallen diverse delicten die kunnen worden onderverdeeld in twee categorieën: cybercriminaliteit en gedigitaliseerde criminaliteit. Wat betreft cybercriminaliteit heeft de minister van JenV uw Kamer een brief gestuurd over de integrale aanpak van cybercrime. In het kader daarvan wordt geïnvesteerd in preventie, wordt de opsporing versterkt, de ondersteuning van slachtoffers meer toegesneden op cybercrime en de wetenschappelijke kennis vergroot.[2]

Omdat over de behoeften van slachtoffers van online criminaliteit, waaronder cybercriminaliteit, nog weinig bekend is, heb ik het WODC gevraagd een verkennend onderzoek te doen naar de impact die slachtoffers van online delicten ervaren, de behoeften van slachtoffers en de verantwoordelijkheden van politie, Openbaar Ministerie (OM) en andere instanties bij de afhandeling van dergelijke delicten. Het Nederlands Studiecentrum Criminaliteitspreventie en Rechtshandhaving (NSCR) heeft op verzoek van het WODC dit onderzoek verricht. Met deze brief bied ik uw Kamer het onderzoeksrapport "Slachtofferschap van online criminaliteit'' en mijn beleidsreactie aan.

**Kern onderzoeksbevindingen**
*Gevolgen van slachtofferschap van online delicten*
Ten behoeve van het onderzoek zijn interviews met 18 Nederlandse experts en 4 internationale experts afgenomen en zijn 19 slachtoffers geïnterviewd. Daarbij is waar mogelijk getracht om slachtoffers van verschillende typen online criminaliteit te interviewen: zowel slachtoffers van cybercrimes (hacken, ransomware), financieel gemotiveerde gedigitaliseerde criminaliteit (phishing, dating fraude), interpersoonlijke gedigitaliseerde criminaliteit (cyberstalking) en online gedigitaliseerde criminaliteit in de zedensfeer (het zonder medeweten of toestemming online delen van seksueel beeldmateriaal). De experts zijn onder meer politiemedewerkers en Officieren van Justitie die zich bezighouden met de opsporing en vervolging van online criminaliteit, maar ook medewerkers van slachtofferhulpinstanties en wetenschappelijk onderzoekers. Uit het onderzoek blijkt dat de meeste gevolgen die slachtoffers van online delicten ervaren,

[1] Tweede Kamer, vergaderjaar 2017–2018, 33 552, nr. 43
[2] Tweede Kamer, vergaderjaar 2017–2018, 28 684, nr. 522

**Directoraat-Generaal Straffen en Beschermen**
Directie Beschermen, Aanpakken en Voorkomen
Cluster slachtofferbeleid

**Datum**
7 februari 2019

**Ons kenmerk**
2492849

overeenkomen met de gevolgen van offline delicten. Zo ervaren de meeste slachtoffers financiële gevolgen en ook melden bijna alle slachtoffers in mindere of meerdere mate psychologische en emotionele gevolgen van online criminaliteit. Door de kenmerken van het online delict kan de impact wel groter zijn. De impact van een online delict kan vergroot worden door de enorme schaal waarop de gevolgen zich kunnen doen gelden, zoals bij het verspreiden van beeldmateriaal. Een bijeffect kan grootschalige *victim blaming* zijn door allerlei onbekenden op het internet.[3] Daarnaast stopt het slachtofferschap niet altijd in tijd. Doordat niemand weet waar op internet kopieën van gegevens en bestanden zijn, is het nooit zeker dat het slachtoffer van de dreiging af is. De ongrijpbaarheid van de meer technische delicten heeft daarnaast als gevolg dat voor slachtoffers onbekend kan blijven wie de mogelijke dader was. Ook kan *victim blaming* vaker voorkomen doordat opsporingsinstanties, hulpverleningsinstanties en de sociale omgeving onbekend zijn met het delict en daardoor het delict niet herkennen of erkennen. Het aanpakken van het delict blijft daardoor soms achterwege.

*Behoeften na slachtofferschap van online criminaliteit*
Uit de interviews blijkt dat slachtoffers van online delicten ook grotendeels dezelfde behoeften hebben als slachtoffers van traditionele offline delicten. De volgende drie behoeften worden het meest belangrijk gevonden: stoppen van slachtofferschap; straf en vergelding; en anderen helpen. In het geval van het zonder medeweten of toestemming online delen van seksueel beeldmateriaal hebben slachtoffers een specifieke behoefte: zij willen het beeldmateriaal zo snel mogelijk offline krijgen. Echter, bij online criminaliteit wordt lang niet altijd in de behoeften van slachtoffers voorzien. Een voorbeeld is de behoefte om als slachtoffer erkend te worden, onder meer door het zorgvuldig opnemen van een aangifte wat nu niet altijd lijkt te gebeuren. Slachtoffers geven ook aan het van belang te vinden dat de dader wordt veroordeeld en dat zij op de hoogte worden gehouden van de voortgang van het opsporingsonderzoek en strafproces. Bij 2 van de 19 geïnterviewde slachtoffers uit het onderzoek is een verdachte gepakt en veroordeeld. De belangrijkste financiële behoefte van slachtoffers is die van vergoeding van schade. In de digitale wereld is het voor één dader mogelijk om zeer veel slachtoffers te maken. Door de mogelijk grote hoeveelheid slachtoffers per dader of groep daders kunnen volgens experts niet alle slachtoffers betrokken worden in het opsporingsonderzoek waardoor ze niet gevoegd kunnen worden in de eis tot schadevergoeding in het strafproces.

## Kabinetsreactie

De integrale aanpak van cybercrime heeft onder andere als doel dat de ondersteuning van slachtoffers wordt toegesneden op cybercrime. Het onderzoek geeft een eerste inzicht in de behoeften van slachtoffers van online criminaliteit, waaronder cybercrime, en welke gevolgen zij ervaren. Uit het onderzoek blijkt niet dat de gevolgen of behoeften van slachtoffers bij online delicten veel afwijken van traditionele delicten. Desalniettemin laat het onderzoek zien dat de impact van online delicten op slachtoffers groot kan zijn. Het is daarom van belang dat slachtoffers zich gehoord voelen door politie, OM en andere instanties. Het onderzoek geeft een indicatie van de knelpunten die slachtoffers van online criminaliteit momenteel ervaren bij de afhandeling van hun zaak. Deze inzichten leiden niet alleen tot nieuwe onderzoeksvragen, maar vormen ook een basis voor de volgende maatregelen die ik wil nemen om slachtoffers van online criminaliteit beter te kunnen helpen:

*Hulpverlening aan slachtoffers van online criminaliteit verbeteren*
Iemand die zich benadeeld voelt, kan op laagdrempelige wijze melding of aangifte

[3] Blaming-the-victim of victim blaming (het slachtoffer de schuld geven) is een vorm van morele ontkoppeling waarbij een dader of omstanders de schuld bij het slachtoffer leggen.

**Directoraat-Generaal Straffen en Beschermen**
Directie Beschermen, Aanpakken en Voorkomen
Cluster slachtofferbeleid

**Datum**
7 februari 2019

**Ons kenmerk**
2492849

doen van online handelsfraude via www.politie.nl. Alle slachtoffers kunnen daarnaast terecht bij Slachtofferhulp Nederland voor praktische, juridische en emotionele hulp. Slachtofferhulp Nederland informeert slachtoffers, zowel offline als online, over rechten en mogelijkheden. Er wordt ondersteuning geboden bij het melden bij relevante instanties en indien mogelijk, het beperken (zoals het verwijderen van beeldmateriaal) en/of verhalen van de schade.
Daartoe werkt Slachtofferhulp Nederland samen met onder meer politie, Fraudehelpdesk, Centraal Meldpunt Identiteitsfraude en –fouten en de hulplijn HelpWanted van het Expertisebureau Online Kindermisbruik (EOKM).

Via het nieuwe online platform van Slachtofferhulp Nederland dat is gelanceerd op 17 april 2018 wordt informatie over de mogelijkheden voor slachtoffers van diverse online delicten verstrekt. Hier staan ook adviezen om (herhaald) slachtofferschap te voorkomen.

- Online vermogensdelicten zoals: identiteitsfraude, fraude met online handel, datingfraude, geldezel, phishing, voorschotfraude, whatsappfraude, skimming, creditboys.
- Online zedendelicten zoals: grooming, sextortion en het zonder toestemming of medeweten delen van beeldmateriaal bij sexting
- Online geweldsdelicten zoals: stalking, bedreiging, cyberbullying / geweld.

Ik financier daarnaast in 2019 een programma van Slachtofferhulp Nederland dat als doel heeft slachtoffers beter te kunnen bedienen door dienstverlening aan te passen aan de individuele behoeften van het slachtoffer. Ik heb Slachtofferhulp Nederland gevraagd hierbij specifieke aandacht te besteden aan de behoeften van slachtoffers van online criminaliteit. Ik zal uw Kamer in het eerste kwartaal van 2020 over de uitkomsten hiervan informeren.

*Herhaald slachtofferschap voorkomen*
Slachtoffer van cybercriminaliteit worden wil niemand, laat staan dat het iemand nogmaals overkomt, of dat iemand nogmaals slachtoffer wordt, maar dan van een ander type cybercriminaliteit. Opvallend is dat slechts de helft van de mensen die slachtoffer zijn geworden van cybercrime (en dat ook weet) actie onderneemt om dat in de toekomst te voorkomen.[4]

Belangrijk onderdeel van voornoemde integrale aanpak van cybercrime betreft het investeren in preventie. In dit kader zal in 2019 een landelijke preventiecampagne van start gaan ter voorkoming van cybercriminaliteit door internetgebruikers. Het doel van de campagne is gebruikers de juiste (preventieve) maatregelen te laten nemen tegen cybercriminaliteit. De campagne richt zich ook op gebruikers die denken dat ze hun online veiligheid al voldoende hebben geregeld of, in dit kader, mensen die eerder slachtoffer zijn geworden van cybercriminaliteit. In de campagne wordt samengewerkt met het bedrijfsleven, omdat het naast een maatschappelijke verantwoordelijkheid ook een belang heeft dat zijn klanten niet (opnieuw) slachtoffer worden van cybercriminaliteit.

De politie geeft daarnaast op haar website www.politie.nl voorlichting over het voorkomen van internetoplichting. Zo kan een potentiële (ver)koper op www.politie.nl controleren of bepaalde gegevens van een mogelijke wederpartij reeds bekend zijn bij de politie.

*Betere bejegening van slachtoffers van online delicten door politie en het OM*
De politie werkt hard om de kennis over cybercrime te vergroten. Inmiddels heeft de politie in alle eenheden cybercrime teams opgericht die ook een bijdrage leveren aan de bewustwording van de Intake- & Servicemedewerkers en kunnen helpen bij het opnemen van aangiftes. Op die manier wordt de kennis bij de

[4] Alert Online, Nationaal Cybersecurity Bewustzijnsonderzoek 2018

politie op gebied van cybercrime vergroot. Daarnaast wordt digitale aangifte dit jaar mogelijk gemaakt voor de cybercrime-delicten ransomware en tech-support scam (in de volksmond de Microsoftfraude genoemd). Hiermee wordt gezorgd dat de politie eenvoudiger bereikbaar is voor slachtoffers van cybercrime.

Slachtoffers hechten belang aan goede informatievoorziening over hun strafzaak en een persoonlijke benadering. Ook slachtoffers van online criminaliteit hechten hier waarde aan blijkt uit het onderzoek. Het OM en SHN willen de ondersteuning verbeteren voor slachtoffers van dergelijke impactvolle zaken die veelal te zwaar zijn voor ZSM, maar ook niet onder de maatwerkaanpak met casemanagement vallen. In dat kader heeft het OM vorig jaar gezamenlijk met SHN in de pilot 'Aandacht voor impactzaken' gekeken naar mogelijkheden om deze groep slachtoffers beter te ondersteunen. De pilot zal in 2019 doorlopen. Een eventuele landelijke invoering in 2020 wordt dit jaar bezien.

*Vervolgonderzoek*
Het hierbij aangeboden onderzoek heeft een kwalitatief, exploratief karakter, en daarvoor is representativiteit van de respondenten niet vereist. Het is een eerste verkenning dat inzichten biedt in de wensen, behoeften en ervaringen van slachtoffers van online criminaliteit in de praktijk, maar er is vervolgonderzoek nodig. Ik heb het WODC in het kader van spoor vier van de integrale aanpak cybercrime gevraagd onderzoek te doen naar oorzaken en gevolgen van online slachtofferschap. Dit is een kwantitatief onderzoek. In dit onderzoek staat centraal hoe vaak bepaalde vormen van online criminaliteit door burgers wordt ervaren, hoe ernstig deze is en wat risicoprofielen zijn van verschillende vormen van online slachtofferschap. Via een panelstudie wordt hierbij gebruik gemaakt van een lange observatieperiode van acht jaar (2010-2018). Naar verwachting wordt dit onderzoeksrapport voor het einde van dit jaar opgeleverd.

De Minister voor Rechtsbescherming,

S. Dekker

**Directoraat-Generaal Straffen en Beschermen**
Directie Beschermen, Aanpakken en Voorkomen
Cluster slachtofferbeleid

**Datum**
7 februari 2019

**Ons kenmerk**
2492849