Gespreksnotitie rondetafelgesprek Publiek Private samenwerking online fraude

Tweede Kamer, Vaste commissie voor Justitie & Veiligheid
Woensdag 1 oktober 2025, 15:00 – 15:45 uur

Spreker: Anne-Jan Oosterheert (Directeur digitale transformatie)

Inleiding

Deze notitie is opgesteld door vertegenwoordigers van de politie ten behoeve van het rondetafelgesprek Publiek Private Samenwerkwerking (PPS) Online Fraude op woensdag 1 oktober 2025. De inhoud geeft weer welke koers de politie heeft ingezet ten aanzien van de digitale transitie en in het bijzonder de PPS. Er wordt ingegaan op wat reeds is bereikt, waar we op dit moment aan werken en waar onze focus ligt.

'Digitale transformatie' is één van de drie grote transformatiethema's van de politie in de Strategische agenda 2025-2030. Onze ambitie is om in 2030 een toonaangevend voorbeeld zijn van een organisatie waar een goede balans bestaat tussen mens en technologie, afgestemd op de maatschappij. Naast investeren in het vermogen om adequaat te reageren op gewijzigde omstandigheden investeren we in ons vermogen om snel en effectief gebruik te maken van moderne technologie met het oog op beter politiewerk en het maatschappelijk effect van politiewerk. Dit vraagt digitale vaardigheid, digitale cultuur en relationeel en digitaal leiderschap.

Met het project 'Operatie Centurion' heeft de politie de afgelopen jaren de aanpak van gedigitaliseerde criminaliteit op vier geprioriteerde vormen[1] van gedigitaliseerde criminaliteit in alle eenheden in werking gebracht. Tussen december 2023 en september 2024 is een externe, onafhankelijke evaluatie van Operatie Centurion gepresenteerd. Op basis van de aanbevelingen is begin 2025 een start gemaakt met het programma Gedigitaliseerde Criminaliteit. Dit programma heeft als doelstelling dat de politie in staat is om Gedigitaliseerde Criminaliteit effectief te bestrijden, waarbij de geleverde inspanningen in verhouding staan tot het nationale en internationale criminaliteitsbeeld. De beoogde effecten daarbij zijn:

- Gedigitaliseerde Criminaliteit met de grootste maatschappelijke impact wordt aangepakt;
- De politie werkt datagedreven samen om de aanpak van Gedigitaliseerde Criminaliteit te optimaliseren;
- Medewerkers van de politie, ketenpartners en PPS werken (inter)nationaal effectief samen aan een gezamenlijke bestrijding van actuele vormen van Gedigitaliseerde Criminaliteit.

Sinds 2016 blijft het slachtofferschap van online criminaliteit stijgen. In 2024 gaven 2,4 miljoen mensen van 15 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van één of meer vormen van online criminaliteit[2]. Ten opzichte van 2022 is dit weer een stijging van ± 9%. Het CBS laat daarbij zien dat jongeren vaker slachtoffer van online criminaliteit zijn dan ouderen. Vooral bij online bedreigingen en intimidatie.

37% van de slachtoffers van online criminaliteit geven het vaakst aan dat zij na het voorval minder vertrouwen hadden in mensen en 30% voelde zich minder veilig. Dit sluit aan bij de bevindingen van het wetenschappelijke promotieonderzoek van Jidau Borwell waarin zij concludeert dat de impact van online criminaliteit verstrekkend kan zijn, op sommige vlakken zelfs ernstiger dan bij klassieke modus operandi. Ruim 40 procent van de respondenten bij het CBS geeft aan behoefte te hebben aan voorlichting over bescherming tegen online criminaliteit.

Publiek Private Samenwerking

Tijdens Operatie Centurion is medio 2022 onder regie van het Ministerie van Justitie en Veiligheid een start gemaakt met de integrale aanpak van online fraude. Een vaste kerngroep en veel andere partners die bij verschillende acties hun expertise ter beschikking stellen[3] hebben hun krachten gebundeld en zijn voortdurend

[1] Online aan- en verkoopfraude, online fraude met betaalproducten, bankhelpdeskfraude en onlinevoorschotfraude
[2] Bron:CBS https://www.cbs.nl/nl-nl/nieuws/2025/16/meer-mensen-slachtoffer-van-online-criminaliteit-in-2024
[3] https://integraleaanpakonlinefraude.nl/page/view/2391c7c7-c9e2-47c7-b776-4bf6d8b615bb/samenwerkingspartners

bezig activiteiten te ontwikkelen om online criminaliteit te verstoren en te stoppen alsmede preventieve acties op te zetten om de inwoners van Nederland te beschermen en weerbaarder te maken. Deze activiteiten betreffen de ontwikkeling van (technische) barrières en interventies voor de meest voorkomende vormen van fraude en vele vormen van voorlichtingsactiviteiten aan o.a. jeugd en senioren.

Voorbeelden daarvan zijn o.a.: in pilotvorm de samenwerking met private partijen om directe aansprakelijkheid toe te passen bij verdachten van online aan- en verkoopfraude; instellen van een checkfunctie op Politie.nl (Check de verkoper); ontwikkelen van een 'nepwebshop (www.pakjedealsnu.nl)'; 'Hack Right", 'Écht niet vandaag!'; Opsporing Verzocht Flits; de integrale stand op de senioren beurzen 'Samen Sterk Tegen Online Fraude', en vele voorlichtingsbijeenkomsten voor senioren. Om de inwoners optimaal te informeren zijn gezamenlijke brochures gemaakt waarin tips staan hoe de veelvoorkomende vormen van online criminaliteit te herkennen en te voorkomen en ook verwijzing naar de instanties waar men terecht kan als men toch slachtoffer geworden is of advies wenst.

De politie zet veel in op de samenwerking met publiek private partijen zoals de Nederlandse Vereniging van Banken, Betaalvereniging Nederland en Currence, Marktplaats, diverse media platformen, Stichting Internet Domein Registratie, telecommaatschappijen en private partijen die zich gespecialiseerd hebben in het verhalen van de schade via het civielrecht. Met enkelen zijn convenanten afgesloten om deze partijen te kunnen activeren maatregelen te treffen als gebleken is van frauduleuze handelen. Online criminaliteit beperkt zich niet tot de landsgrenzen. Het is zeer voor een EU-ingezetene eenvoudig buitenlandse bankrekeningen te openen en via 'instant payments' direct geld daarop te storten. De tijdsduur die thans aan internationale rechtshulpverzoeken verbonden zit om instant informatie te bevragen maakt het mogelijk dat dat de gelden al opgenomen/ doorgesluisd zijn en is het maar de vraag of de rekeninghouders vindbaar zijn. Een Europees Verwijzingsportaal Banken is reeds in ontwikkeling. In het meest gunstige geval is de planning dat deze in 2029 in werking gaat. Gezien het criminaliteitsbeeld op dit gebied is het nu al wenselijk dat het Europees Verwijzingsportaal Banken in werking is. Een kans op korte termijn zou een pilot zijn met een EU-land waar veel bankrekeningen worden geopend die worden ingezet voor fraude.

De integrale samenwerking laat zien dat partijen elkaar versterken in de totale aanpak. Knelpunt is echter de beperking die de Algemene Verordening Gegevensbescherming (AVG) aan de partijen oplegt om gegevens met elkaar te delen. Door deze beperkingen is het nu zeer moeilijk om met banken en telecommaatschappijen initiatieven om technische barrières en interventies te ontwikkelen. De behoefte hieraan is groot omdat door deze interventies en barrières veel slachtoffers van online criminaliteit kunnen worden voorkomen.
Daarnaast moeten slachtoffers van online criminaliteit nu vaak op meerdere plaatsen hun verhaal vertellen (bij de banken, de Fraudehelpdesk (FHD), de politie, en Slachtofferhulp Nederland). De AVG staat in veel gevallen niet toe dat samenwerkingspartners de gegevens met elkaar delen. Dit leidt ertoe dat een groot deel van de slachtoffers na eenmaal een melding bij de bank of FHD te hebben gedaan afzien doen van aangifte. Het CBS heeft onderzocht dat bijna 2 op de 10 slachtoffers van online criminaliteit melding en aangifte bij de politie. De meest genoemde reden om het voorval niet bij de politie te melden of geen aangifte te doen is dat men er niet aan heeft gedacht of het niet zo belangrijk vond, gevolgd door 'het helpt toch niets'. Om de aangiftebereidheid te vergroten, opsporingskansen te verbeteren en technische barrières en interventies in te stellen is het wenselijk dat de mogelijkheden tot het uitwisselen van data onder samenwerkingspartners worden vergroot. Als voorbeeld kan hiervoor het Digitaal Patiëntendossier dienen waar, na toestemming van de betrokkene, gegevens worden gedeeld met vooraf geduide samenwerkingspartners.

Samenwerking met de Fraudehelpdesk
De FHD adviseert, indien relevant, haar melders melding te maken of aangifte te doen bij de politie. Voor veel slachtoffers zijn zij het eerste contact nadat zij target zijn geweest of slachtoffer zijn geworden van online criminaliteit. Mensen die kennis hebben van strafbare feiten waar zij mee geconfronteerd zijn, ervaren echter (soms onoverkoombare en hiervoor beschreven) drempels om deze gegevens onder de aandacht te brengen van de politie. Soms omdat het ze te veel moeite is ondanks adviezen in deze richting maar deels ook doordat het lastig en soms onmogelijk is de informatie in te brengen.

Dit leidt tot o.a.:

- Teleurstelling/ontevredenheid onder die mensen;
- Aantasting van vertrouwen in de politie en de rechtstaat in zijn algemeen;
- Aantasting van aangiftebereidheid;
- Obstructie van inname van voor de opsporing relevante gegevens.

Pilot

Als proef heeft in 2025 een medewerkster van de politie uit de eenheid Oost-Nederland 5 maanden haar werkzaamheden op de FHD verricht. Het doel was te onderzoeken of deze werkwijze zou leiden tot betere hulpverlening aan slachtoffers, betere informatiedeling (met inachtneming van de geldende privacyregels) en een efficiëntere inrichting van onze werkprocessen. Deze pilot is geëvalueerd en er is gezamenlijk (politie en FHD) geconcludeerd dat de dienstverlening in het kader van de samenwerking tussen de politie en de FHD door deze inzet sterk verbeterd is. Met name het vergemakkelijken van het aangifteproces voor de melder, de kortere doorlooptijd in de afhandeling van de melding en de efficiëntie van een warme overdracht heeft ertoe geleid dat de klanttevredenheid aanzienlijk is verbeterd in de casussen waarbij een goede samenwerking tussen politie en FHD vereist is. Gezien dit resultaat is besloten om voor de komende twee jaar een vervolg op deze pilot te geven. Hierbij wordt de bezetting uitgebreid met drie politiemedewerkers die ons in staat stellen om het gebied, van waaruit we melders kunnen helpen, uit te breiden van Oost-Nederland (Gelderland en Overijssel) naar heel Nederland.

Naast de samenwerking met de eenheid Oost-Nederland werkt het Landelijk Meldpunt Internet Oplichting ook al geruime tijd samen met de FHD. Voorbeelden daarvan zijn:

- Het openstellen van de API naar de checkfunctie op politie.nl. Via de checkfunctie kunnen burgers controleren of er meldingen zijn gedaan tegen vier specifieke entiteiten, namelijk een bankrekeningnummer, een telefoonnummer, een emailadres en een URL (Uniform Resource Locator) van een webpagina;
- Campagnes ten behoeve van het voorkomen van slachtoffers van gedigitaliseerde criminaliteit. Zo is er vorig jaar in samenwerking met de FHD een nepwebshop gelanceerd vanuit de politie (www.pakjedealsnu.nl) en is een nieuwe nepwepshop in ontwikkeling;
- Het ontwikkelen van een vragenboom waarmee (potentiële) slachtoffers middel een advies worden doorgeleid naar de juiste partijen voor het doen van een melding/ aangifte en zij een duidelijk handelingskader krijgen in welke stappen zij verder kunnen ondernemen. Denk bijvoorbeeld aan de PNBF-procedure (verkrijging NAW-gegevens van de wederpartij van de bank) en advies over de partijen die hen hierbij kunnen ondersteunen (SODA/LAVG/AGN). Dit advies krijgt een (potentieel) slachtoffer ook toegezonden via de mail en indien gewenst kan een slachtoffer gebeld worden voor verder advies of ondersteuning;
- Het notificeren van malafide websites aan de FHD, zodat de FHD via hun eigen kanalen kan waarschuwen voor deze sites.

Tot slot

Online Criminaliteit blijft groeien en criminaliteitsvormen worden door AI steeds moeilijker te onderkennen. Het blijft de komende jaren dus zaak om in PPS de inwoners van Nederland weerbaar te maken, te blijven investeren op het vergroten van de aangifte bereidheid, de opsporing en het ontwikkelen van barrières en interventies.