Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

29 911 Bestrijding georganiseerde criminaliteit

Nr. 489

VERSLAG VAN EEN RONDETAFELGESPREK

Vastgesteld 7 november 2025

De vaste commissie voor Justitie en Veiligheid heeft op 1 oktober 2025 gesprekken gevoerd over **onlinefraude**.

Van deze gesprekken brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de commissie,
Pool

De griffier van de commissie,
Brood

kst-29911-489
ISSN 0921 - 7371
's-Gravenhage 2025

Voorzitter: Van Nispen
Griffier: Van Tilburg

Aanwezig zijn vijf leden der Kamer, te weten: Michon-Derkzen, Mutluer, Van Nispen, Six Dijkstra en Wijen-Nass,

alsmede mevrouw Bongers, mevrouw Buisman, mevrouw Galič, mevrouw Van 't Hoff, mevrouw Junger, mevrouw Van der Laan, mevrouw Mieremet, mevrouw Molenaar, de heer Nijhof, de heer Oosterheert, mevrouw Sander en de heer Wolfsen.

Aanvang 14.07 uur.

De **voorzitter**:
Goedemiddag. Ik open dit rondetafelgesprek van de vaste Kamercommissie voor Justitie en Veiligheid over het thema onlinefraude. Dat thema stond op onze kennisagenda, waarvoor we als rapporteurs mevrouw Michon-Derkzen en de heer Six Dijkstra hadden. Waarvoor dank, en zeker ook aan de ondersteuning die ons daarbij geholpen heeft.

Blok 1: Wetenschap/experts

Gesprek met:
– Marianne Junger, professor of Cyber Security and Business Continuity, Universiteit Twente, schrijver wetenschappelijke factsheet
– Sanne Buisman, associate professor, Vrije Universiteit Amsterdam, schrijver wetenschappelijke factsheet
– Maša Galič, assistant professor, Vrije Universiteit Amsterdam, schrijver wetenschappelijke factsheet
– Susanne van 't Hoff-de Goede, associate lector Cybercrime & Cybersecurity, Haagse Hogeschool

De **voorzitter**:
In dat kader zijn ook twee factsheets opgesteld. Ik ga meteen onze gasten in het eerste blok van harte welkom heten. Er is onder andere een factsheet opgesteld door mevrouw Marianne Junger, professor of Cyber Security and Business Continuity aan de Universiteit Twente. Mevrouw Buisman en mevrouw Galič hebben ook een factsheet opgesteld. Mevrouw Buisman is associate professor aan de Vrije Universiteit en mevrouw Galič is assistant professor, ook aan de Vrije Universiteit. Daarnaast hebben we mevrouw Van 't Hoff-de Goede te gast, associate lector Cybercrime & Cybersecurity bij de Haagse Hogeschool. Goed dat u er allemaal bent en dat u ons wilt bijspijkeren op dit belangrijke thema. Excuses dat we te laat starten. Dat heeft alles te maken met de hoofdelijke stemming in de plenaire zaal, maar daar was u over geïnformeerd. We gaan snel van start. Ik geef het woord aan mevrouw Junger om als eerste een toelichting te geven.

Mevrouw **Junger**:
Dank u wel, voorzitter. Dank voor de uitnodiging. Een derde van alle incidenten in de politiegegevens betreft onlinefraude. Fraude is het best te omschrijven als een crimescript, een stapsgewijs plan dat ontstaat op 1.001 plekken. Eén fraude-incident komt langs bij meerdere organisaties. Het kan starten op social media en naar de onlinemarkten gaan. Het maakt gebruik van telecombedrijven, gaat naar verschillende banken en het geld wordt razendsnel doorgesluisd. Kennis over fraude raakt versnipperd, niemand heeft het totaaloverzicht en de overheid dreigt grip te verliezen op het fenomeen. Het goede nieuws is dat preventie helpt. In relatie tot preventie wordt vaak verwezen naar het zogenaamde waterbedeffect. Hoewel dit zeker soms voorkomt, is het zeker niet absoluut. Online-

interventies en preventieve maatregelen kunnen effectief zijn en arrestaties zijn uiteraard ook nuttig.
Ik geef enkele voorbeelden uit het buitenland. Ten eerste. De Australische regering heeft in een alomvattend plan alle betrokkenen meer verantwoordelijkheid gegeven. Banken moeten aanvullende controles implementeren. Telecombedrijven moeten frauduleuze oproepen en berichten beter detecteren en verstoren. Socialmediabedrijven zullen frauduleuze advertenties moeten verwijderen en moeten zorgen voor een betere apparaatauthenticatie. Ook is er een antifraude-informatiesysteem ontwikkeld, waarmee banken, telecomnetwerken, internetproviders en socialmediabedrijven informatie delen om fraude gezamenlijk te bestrijden. In één jaar daalde het aantal incidenten met 18% en daalden de verliezen met 26%. Het is belangrijk om gegevens te delen onder de juiste voorwaarden, maar ik denk dat snelle en efficiënte beroepsprocedures voor degenen die onterecht als fraudeur zijn bestempeld vooral belangrijk zijn.
Het tweede voorbeeld: het VK. Daar vergoeden de banken nu alle verliezen als gevolg van fraude. Deze compensatie wordt fiftyfifty verdeeld tussen de verzendende en de ontvangende bank. Dit leidde tot een daling van het aantal claims met een derde in de eerste vier maanden na ingang van het beleid. Cifas, het platform voor gegevensdeling in het VK, heeft in 2019 naar schatting gezorgd voor het voorkomen van 1,5 miljard pond aan fraude.
In de factsheet benadruk ik ook het belang van opsporing en proactieve educatie van gebruikers. Mevrouw Van 't Hoff zegt hier straks geloof ik ook iets over.
Dan de opsporing. Veel problemen zijn nieuw. Experimenteerruimte voor nieuw beleid is belangrijk, om uit te zoeken wat effectief is en wat niet. Dit geldt voor de politie en waarschijnlijk ook voor andere organisaties. De laatste cijfers voor het VK laten zien dat fraude afneemt, volgens de financiële sector. Een geïntegreerde aanpak, samenwerking en het delen van gegevens leiden tot effectiever en efficiënter beleid. Daartoe lijkt het nuttig een centrale organisatie verantwoordelijk te maken. U zou een nationaal fraudebestrijdingscentrum kunnen oprichten, naar Australisch voorbeeld. U zou de Fraudehelpdesk daarvoor als startpunt kunnen gebruiken. U zou ook een Minister voor Fraudebestrijding kunnen aanstellen, naar het voorbeeld van het VK.
Dank u wel.

De **voorzitter**:
Hartelijk dank voor uw toelichting. Dan geef ik het woord aan mevrouw Galič.

Mevrouw **Galič**:
Geachte voorzitter. Dank voor deze mogelijkheid om onze factsheet inzake de opsporing en vervolging van onlinefraude onder het huidige en nieuwe Wetboek van Strafvordering nader toe te lichten. Onlinefraude is een containerbegrip voor allerlei vormen van bedrog gericht op financieel gewin die zonder ICT niet mogelijk zouden zijn geweest. Daarbij kan worden gedacht aan verkoopfraude, bankhelpdeskfraude, betaalverzoekfraude, bankphishing enzovoort. Onder het Wetboek van Strafrecht worden diverse strafbepalingen gebruikt om onlinefraude te vervolgen, zoals computervredebreuk, oplichting, witwassen en valsheid in geschrifte. Deze strafbaarstellingen maken het mogelijk om meer ingrijpende opsporingsbevoegdheden in te zetten om verdachten van deze strafbare feiten op te sporen. De huidige capaciteit binnen de strafrechtketen is echter beperkt tot een kleine 7.000 zaken per jaar op het terrein van gedigitaliseerde criminaliteit, terwijl de omvang van onlinefraude vele malen groter is. Het gaat om 1,4 miljoen slachtoffers in 2024.

Strafrechtelijk ingrijpen is bovendien slechts een reactie. Het wordt pas ingezet als er al een strafbaar feit is gepleegd. Het is om die reden dat bij de bestrijding van onlinefraude wordt ingezet op een integrale aanpak. Met deze aanpak wordt onder meer ingezet op preventie en samenwerking met publieke en private partners om onlinefraude te bestrijden. Daarbij kan uit verschillende interventies binnen de verschillende deelterreinen worden geput. Denk aan het privaatrecht, het bestuursrecht en het tuchtrecht, maar ook aan campagnes en hulpverlening. Een dergelijke samenwerking is alleen mogelijk als er wordt geïnvesteerd in de samenwerking tussen politie en justitie en de publieke en private partners, alsook in de gegevensuitwisseling tussen deze partijen. De beperkte capaciteit en het reactieve karakter van het strafrecht nopen er ook toe dat er keuzes worden gemaakt ten aanzien van het type zaken dat via het strafrecht wordt afgedaan.
In dat kader zou, mede in het licht van het ultimumremediumkarakter van het strafrecht, de inzet van het strafrecht moeten worden beperkt tot de meest ernstige gevallen van onlinefraude, zoals gevallen met een groot aantal slachtoffers, een hoog schadebedrag, een georganiseerd verband of complexe casussen. Wanneer een zaak de inzet van het strafrecht rechtvaardigt, biedt het huidige Wetboek van Strafvordering een groot aantal bevoegdheden waarvan gebruik kan worden gemaakt bij de opsporing van onlinefraude. Vanwege het digitale karakter van deze vorm van criminaliteit betreft het in de meeste gevallen dan ook digitale opsporingsbevoegdheden.
De belangrijkste bevoegdheden zijn: het vorderen van identificerende en verkeersgegevens, doorzoeking van geautomatiseerde werken, netwerkzoeking tijdens het doorzoeken van plaatsen en aftappen van communicatie. Daarnaast zijn bevoegdheden inzake het ontoegankelijk maken van gegevens van belang bij de bestrijding van onlinefraude. Onder het nieuwe Wetboek van Strafvordering wordt de regeling voor digitale opsporing volledig geherstructureerd, waarbij het onderzoeken van gegevens een centrale positie krijgt. De inzet van deze bevoegdheid wordt genormeerd aan de hand van het stelselmatigheidscriterium. Hoe ingrijpender de inbreuk op het privéleven van een persoon, hoe preciezer de bevoegdheid moet zijn geformuleerd en hoe hoger de functionaris is die de toepassing van bevoegdheden moet goedkeuren.
Onder het nieuwe Wetboek van Strafvordering worden ook een aantal nieuwe opsporingsbevoegdheden geïntroduceerd die relevant kunnen zijn voor de opsporing van onlinefraude. Het gaat daarbij om het kennisnemen van gegevens na inbeslagname en netwerkzoeking na inbeslagname, waarmee reeds ervaring is opgedaan onder de Innovatiewet Strafvordering en waarvan de evaluaties grotendeels positief zijn. Tevens kunnen het bevel tot data-analyse door een derde en stelselmatige locatiebepaling van belang zijn in de opsporing van onlinefraude. Daarmee lijken er afdoende mogelijkheden te bestaan om ernstige gevallen van onlinefraude op te sporen en vervolging daarvan zeker te stellen. Een kanttekening is wel dat de aanwezigheid van een grensoverschrijdend aspect de opsporing kan bemoeilijken, omdat in die gevallen justitiële samenwerking met het buitenland noodzakelijk is. Dit probleem wordt wel gedeeltelijk aangepakt met de komende e-Evidenceverordening en -richtlijn.
Tot slot. Zoals ik hiervoor al heb aangegeven, is in het kader van de integrale aanpak van onlinefraude de uitwisseling van persoonsgegevens van groot belang. Dit was niet het onderwerp van onze factsheet, maar verdient onzes inziens niettemin enige aandacht, omdat gegevensbeschermingsrecht, waaronder de AVG, soms wordt gezien als een obstakel in de bestrijding van onlinefraude. Dat is volgens ons echter een misvatting. De AVG staat het uitwisselen van persoonsgegevens voor de bestrijding van onlinefraude toe, mits deze verwerking van persoonsgegevens op een rechtmatige en legitieme manier gebeurt. De verwerking van persoonsge-

gevens in een mogelijk strafrechtelijke context kan immers aanzienlijke gevolgen hebben voor alle betrokken personen. In het volgende panel wordt dit onderwerp ook verder besproken.
Dank voor uw aandacht. We kijken uit naar de verdere gedachtewisseling.

De **voorzitter**:
Dank u wel, mevrouw Galič. Dat was meteen namens u, nietwaar, mevrouw Buisman? Als er straks vragen zijn, kunt u zelf kijken wie van u beiden ze beantwoordt als ze aan uw adres zijn. Dan geef ik het woord aan mevrouw Van 't Hoff-de Goede.

Mevrouw **Van 't Hoff**:
Geachte voorzitter, geachte leden van de commissie, hartelijk dank voor de uitnodiging om hier aanwezig te zijn. Mij is gevraagd niet een factsheet maar een gespreksnotitie op te stellen, waarin ik ervaringen en vooral aanbevelingen die ik zou willen doen, uiteenzet, gebaseerd op zeven jaar onderzoek naar slachtofferschap van onlinecriminaliteit.
Ik start met de kleine uiteenzetting dat in 2024 1,4 miljoen Nederlanders online werden opgelicht. Wij zien in wetenschappelijk onderzoek dat de impact daarvan niet alleen groot is, maar ook dat de gerapporteerde mentale gevolgen geregeld groter zijn dan de financiële. Fraudeurs gaan zo gewiekst te werk dat iedereen – ik wil graag een streep zetten onder «iedereen», inclusief mezelf – slachtoffer van onlinefraude kan worden. Dat beeld is niet nieuw en komt al jaren naar voren in onderzoek. Toch worden er nog veel te weinig stappen gezet om onlinefraude terug te dringen en burgers te beschermen. Wetenschappelijk onderzoek wijst op diverse mogelijke stappen, waarvan ik er zo veel mogelijk in twee bladzijden heb geprobeerd uiteen te zetten, gegroepeerd in drie thema's.
Het eerste thema is preventie. Die zou ik dan het liefst gericht willen zien op vier subgroepen. De eerste is gericht op slachtoffers. Een van de grootste risicofactoren voor slachtofferschap die wij in wetenschappelijk onderzoek namelijk zien, is slachtofferschap, oftewel herhaald slachtofferschap. Slachtoffers van onlinefraude lopen meer of veel meer risico dan anderen om opnieuw slachtoffer te worden, zowel van hetzelfde als van een ander delict. Hoewel er veel meer onderzoek nodig is om te verklaren welke achtergrondfactoren dit verband veroorzaken, zou er reeds ingezet moeten worden op de ontwikkeling van wetenschappelijk onderbouwde preventieve interventies gericht op herhaald slachtofferschap. Deze slachtoffers melden zich ergens en dat is een uitgelezen moment om hierop in te stappen.
De tweede groep is gericht op potentiële slachtoffers. Fraudeurs lichten mensen op door middel van social engineering. In vele vormen van fraude worden dezelfde manipulatietechnieken gebruikt. We kunnen daarmee fraude voorkomen door mensen weerbaar te maken. Daarbij vallen we ook niet in de kuil dat we mensen weerbaar maken voor een delict dat er een jaar later heel anders uitziet, als we focussen op de achterliggende sociale, psychologische mechanismen. Daarbij is het van groot belang dat interventies en campagnes die zich richten op gedragsverandering, verder gaan dan het vergroten van awareness. Meer kennis leidt niet automatisch tot veiliger gedrag. Wij zien in wetenschappelijk onderzoek zelfs dat mensen met meer kennis van onlineveiligheid zich online eerder ónveiliger gedragen. We moeten dus veel verder gaan dan awareness en kennis als we op preventie willen inzetten. We moeten daarbij ook inzetten op digitale geletterdheid. Eigenlijk vanaf de leeftijd dat we gaan lopen en praten, zou dat onderdeel moeten zijn van preventie. Verder moeten we inzetten op weerbaarheid in het onderwijs en daarbuiten.
De derde groep is gericht op systemen en het betaalverkeer. Ondanks dat mijn vak zich richt op de menselijke factor in cybercriminaliteit, durf ik ook te stellen dat interventies gericht op het gedrag van potentiële slachtoffers

en slachtoffers nooit afdoende zullen zijn. Er moet worden ingezet op technische maatregelen tegen onlinefraude. We moeten mensen in bescherming nemen, bijvoorbeeld door gebruik te maken van security by design, door het beveiligen van systemen, of door waar mogelijk bijvoorbeeld anoniem betaalverkeer tegen te gaan.
De vierde groep is gericht op daders en criminele netwerken. Hoewel dit niet mijn corebusiness is, gebeurt er op dit thema belangrijk werk, onder andere in onze onderzoeksgroep. Ook door de inzet op preventie van daderschap en het ezelen van geld kunnen we slachtofferschap voorkomen.
Deze interventies moeten bovendien wetenschappelijk worden onderbouwd en geëvalueerd. Dat wil ik ook graag nog even benadrukken. Daarbij zou het goed zijn als er meer gebruik wordt gemaakt van de kennis die er al is, want er is al veel meer bekend dan de kennis waar nu gebruik van wordt gemaakt. Zet onderzoekers bovendien in bij het evalueren en zet in op een evidencebased doorontwikkeling.
Mijn tweede thema, na preventie, is de zorg voor slachtoffers. Elke Nederlander moet weten wat te doen in geval van fraude. Gegeven dat elk jaar 16% slachtoffer is, lopen we allemaal een groot risico. Veel Nederlanders kennen de eerste belangrijke stap nog helemaal niet, namelijk het bellen van je bank. Vaak is ook het noodnummer dat ook buiten kantooruren bereikbaar is voor hen onbekend. Zo sprak ik bijvoorbeeld een slachtoffer dat zei: ik werd op vrijdagavond opgelicht, dus ik moest tot maandag 09.00 uur wachten voordat ik hulp kon vragen. Pas als het algemeen bekend is en slachtoffers zich daadwerkelijk hier melden, kunnen betaaldienstverleners waar mogelijk ingrijpen en slachtoffers vervolgens doorverwijzen naar hulporganisaties voor hulpverlening, aangifte en/of registratie.
Er is een breed scala aan organisaties die klaarstaan voor slachtoffers. Laat ik benadrukken dat dit heel mooi is, maar dat heeft tevens het ongewenste neveneffect dat slachtoffers niet altijd weten waar ze het beste terechtkunnen. Oftewel, ze zien als ze hulp zoeken bij onlinefraude door de bomen het bos niet. De keten van partijen moet niet alleen samenwerken, maar ook samen optreden richting slachtoffers. Dat zou bovendien behoeftegestuurd moeten worden aangeboden. Behoeften van slachtoffers lopen namelijk sterk uiteen.
Een mogelijke route voor genoegdoening van slachtoffers van onlinefraude loopt via het civiel recht, buiten het strafrecht. Daarbij vorderen slachtoffers het verloren geld terug van de ontvanger van het geld. Momenteel wordt door mijzelf en collega Merel van Leuken een grootschalig onderzoek uitgevoerd naar de werking en gevolgen van deze aanpak van onlinefraude. Diverse deelrapporten zijn openbaar. De eindpublicatie volgt in 2026.
Tot slot wil ik binnen dit thema zeggen: overweeg vergoeding voor slachtoffers vanuit een fonds of betaal dienstverleners. Leer daarbij van buitenlandse voorbeelden, zoals Marianne Junger ook al zei. Een voorbeeld is de vergoeding die banken in het VK vorig jaar hebben ingevoerd.
Mijn laatste thema heeft te maken met zicht op fraude. Voor de aanpak van onlinefraude is eerst inzicht nodig. Hiervoor moet de meldingsbereidheid van slachtoffers worden vergroot en de niet-melders moeten ook worden bereikt en indien gewenst doorverwezen. Een van de redenen dat slachtoffers zich niet melden of geen hulp zoeken, is victimblaming. Een recent onderzoek wijst uit dat blaming en selfblaming in hogere mate bij onlinecriminaliteit plaats zou kunnen vinden dan bij traditionele criminaliteit. Bekenden geven slachtoffers de schuld: «Hoe heb je dat nou kunnen doen?» Dit horen ze niet alleen van bekenden, maar zelfs van professionals waar ze naartoe gaan voor hulp: de politie en andere organisaties. Bovendien geven slachtoffers zichzelf ten onrechte de schuld van wat hun

is overkomen. Dat vergroot niet alleen de impact, maar verkleint ook de bereidheid om zich te melden en hulp te zoeken.
Ik wil eindigen door te zeggen dat er veel meer onderzoek nodig is naar dit thema, naar slachtofferschap en weerbaarheid van onlinefraude. Er is ook mooi nieuws: wij zijn deze zomer gestart met een vierjarig onderzoeksprogramma, genaamd Weerbaar tegen online criminaliteit. Daarbij gaan we ons met de Haagse Hogeschool en Hogeschool Saxion in opdracht van Fonds Slachtofferhulp en het Ministerie van Justitie en Veiligheid richten op enkele van deze thema's.
Dank u wel.

De **voorzitter**:
Dank u wel. Dank aan u allen voor deze wijze woorden waar we ons voordeel mee kunnen gaan doen. Maar er zijn ongetwijfeld vragen. Ik stel voor om even te beginnen met één vraag per persoon. Dan kunnen we vast meerdere rondjes doen. Ik wil de vragen graag eerst eventjes verzamelen. Dat zullen er vier of vijf worden. Zeg er vooral bij aan wie u de vraag richt. Allereerst geef ik het woord aan de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Dank u wel, voorzitter. Veel dank voor uw komst, veel dank voor uw toelichting en voor het schrijven van uw factsheets. Het is een zeer relevant onderwerp. Het heeft grote maatschappelijke urgentie om hier wat aan te doen, dus het is fijn om het hier met elkaar over te kunnen hebben. Mijn eerste vraag kan ik het beste richten aan mevrouw Galič en/of mevrouw Buisman. Die gaat over het principe van massaslachtofferschap. Het gaat vaak om criminaliteit die soms hele grote groepen slachtoffers kan hebben. Dat sluit niet altijd natuurlijk aan bij de manier waarop wij ons strafproces hebben ingericht. Ik ben benieuwd of u uw visie kunt geven op de vraag hoe beleid of wetgeving eventueel nog aangepast zou moeten worden om misschien meer te faciliteren dat strafzaken met heel veel slachtoffers, zoals onlinefraude, ook beter voor de rechter gebracht zouden kunnen worden.

De **voorzitter**:
Dank u wel. De vraag van mevrouw Michon-Derkzen.

Mevrouw **Michon-Derkzen** (VVD):
Voorzitter. Ook namens mij hartelijk dank. Het is heel waardevol dat we het hier vanmiddag over hebben. Ik zou graag een vraag willen stellen over het daderschap en het aanpakken van de daders. Ik kijk naar de dames Buisman en Galič. Ik hoop dat ik bij u aan het goede adres ben. Ik hoorde u ook zeggen dat het vaak over landsgrenzen heen gaat. Dan bekruipt me het gevoel dat we nog met ouderwetse maatregelen vanuit Strafvordering een heel nieuw fenomeen proberen aan te pakken. Hoe zou je volgens u de daders hierop beter aan kunnen pakken en hoe zou je effectiever in internationaal verband kunnen optreden?

De **voorzitter**:
Mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Ik moest naar aanleiding van de woorden van mevrouw Van 't Hoff-de Goede dat het iedereen kan overkomen, denken aan het appje dat ik twee dagen terug van mijn zogenaamde «zoon» kreeg. Die was zijn telefoon kwijt en vroeg aan diens vader, die ik niet ben, of hij geld kon overmaken. Dat was niet de eerste keer, want volgens mij liggen onze telefoonnummers ook ergens bij criminelen die daar misbruik van maken. Mijn vraag – ik kijk gelijk naar mevrouw Van 't Hoff-de Goede – gaat over slachtofferschap. Ik heb eerder een voorstel ingediend om de

PNBF-regeling, de procedure begunstigde naw-gegevens bij niet-bancaire fraude, waarvan de naam natuurlijk veranderd moet worden, veel meer onder de aandacht te brengen. Daarmee kunnen namelijk onder andere de naw-gegevens aan de slachtoffers worden verstrekt. Die kunnen daarmee dan vervolgens onder andere naar een deurwaarder gaan. Dat is een soort interbancaire regeling. De overheid doet daar niets mee, maar ik hoor jullie toch allemaal, overigens ook mevrouw Junger, zeggen dat je een veel integralere aanpak nodig hebt. Dus hoe kijken jullie naar de ineffectiviteit en de leemtes van de regelingen die we nu hebben?

De **voorzitter**:
Dank u wel. Mevrouw Wijen-Nass.

Mevrouw **Wijen-Nass** (BBB):
Dank u wel, meneer de voorzitter. Ook dank namens mij voor jullie aanwezigheid vandaag en de toelichting. Het ging er ook over dat er nu zo'n 7.000 zaken zijn, terwijl er iets van 1,4 miljoen slachtoffers waren in 2024. Uit de bijdragen leek ik te begrijpen dat we juridisch op zich wel voldoende zijn toegerust om de daders te kunnen aanpakken. Ik vroeg me nu af: zit het 'm er vooral in dat er toch minimaal aangiftes worden gedaan, of zit het 'm in de capaciteit? Of zit het 'm erin dat we toch te maken hebben met criminelen die makkelijk de grens overgaan? Ik was dus een beetje aan het zoeken naar de vraag hoe we meer van die daders gaan pakken.

De **voorzitter**:
Had u al gezegd aan wie u uw vraag richtte?

Mevrouw **Wijen-Nass** (BBB):
Nee, aan wie het wil.

De **voorzitter**:
U moet altijd oppassen dat het dan niet drie vragen zijn, maar we zitten volgens mij goed in de tijd.
Ik zou daar zelf nog één vraag aan toe willen voegen. Ik stel die aan mevrouw Junger. In een van uw eerste zinnen waarschuwde u voor het risico dat kennis over fraude versnipperd raakt. Ik vroeg me toen af of dat dan onvermijdelijk is. U sloot eigenlijk af door te zeggen dat je naar een nationaal fraudebestrijdingscentrum toe zou moeten, bijvoorbeeld naar Australisch voorbeeld, maar u noemde ook het Verenigd Koninkrijk. Ik zou u toch willen uitdagen om dat nog nader toe te lichten, want dat is een idee dat niet voor het eerst is opgekomen. Dat idee is hier in de Tweede Kamer ook al weleens eerder geopperd, maar kunt u nader onderbouwen waarom dat volgens u nu zo noodzakelijk is?
Heeft u de vragen genoteerd? De smokkelvraag van mevrouw Wijen-Nass die aan u allemaal is gesteld, mag u daarbij betrekken. Ik ga, denk ik, gewoon weer het rijtje af. Ik begin bij mevrouw Junger.

Mevrouw **Junger**:
Dan gaat het eerst over de naw-gegevens, geloof ik? Ik heb begrepen dat dat een experiment is dat op dit moment bij de politie loopt. Dat is een experiment om te bekijken hoe het allemaal loopt als de gegevens aan de slachtoffers worden verschaft. Veel van deze problemen zijn relatief nieuw. We moeten nog leren hoe we ermee omgaan. Het is een interessant experiment om die gegevens te verschaffen en dan te kijken of je op die manier met een soort van snellere procedure je geld terug kunt krijgen. Wat volgens mij verstandig is, is het volgende. Je hebt een goed idee. Je gaat het uitproberen. Je doet dat in de praktijk. Je probeert dat goed te evalueren. Je gaat het invoeren als het werkt. Eventueel pas je het aan. Dat is het dan. U had wat anders in gedachten?

Dan zeg ik nog iets over dat nationale fraudecentrum. Op dit moment hebben de banken een beleid en heeft de politie een beleid. Wellicht heeft het Openbaar Ministerie nog eigen aandachtspunten. Fraude is ook overal. De onlinewinkels hebben ook iets van informatie. Die zullen hun eigen zwarte lijsten hebben van mensen die niet betalen. Je zou die coördinatie willen en de richting van wat je dan gaat doen om dat beleid te coördineren. Blijkbaar heeft dat in Australië goed gewerkt, want daar hadden ze een afname van 18% van het aantal zaken en een afname van 26% van de schade. Op dit moment werkt het toch niet helemaal goed genoeg. Zo zou je het kunnen zeggen. Het interessante is dat door de preventieve maatregelen die bedrijven van 2016 tot 2024 hebben genomen, het slachtofferschap bij die bedrijven echt is afgenomen. Bij individuen die kwetsbaarder zijn en minder maatregelen nemen, is sprake van de omgekeerde beweging: steeds meer slachtofferschap. Als we daar iets aan willen doen, moeten we toch iets aan dat beleid doen. Aan de laatste cijfers van UK Finance zie je dat het in Engeland, waar ze er nog veel meer last van hebben dan wij, echt aan het afnemen is. Ik vind dat een sterk verhaal. Dat is het algemene idee.

De **voorzitter**:
Dan kijk ik naar mevrouw Buisman.

Mevrouw **Buisman**:
Ik neem de vraag over het massaslachtofferschap voor mijn rekening. Het is volgens mij ergens in 2018 geweest toen voor het eerst de bepaling voor onlinehandelsfraude werd ingevoerd. Er was veel discussie over de vraag wanneer je die inzet. Onder andere in de parlementaire discussie werd daarover aangegeven dat daar een selectie van zaken in moet komen, omdat er heel veel gevallen van Marktplaatsoplichting zijn en we die niet allemaal kunnen vervolgen of überhaupt opsporen. Toen was er een soort van indicatie, nattevingerwerk, dat we bij 180 aangiftes eens zouden gaan kijken of het een zaak zou zijn waarvoor opsporing en vervolging in beeld zouden moeten komen. Als je zelf het Openbaar Ministerie over hun ervaringen met vervolging van internetoplichting hoort, dan geven ze aan dat die zaken juist vanwege het massaslachtofferschap heel lastig zijn om bij de strafrechter aan te brengen. Dat is juist omdat de zaak zelf inhoudelijk niet heel ingewikkeld is, maar het strafproces ook de mogelijkheid biedt om je te voegen als benadeelde partij en daarbij binnen die strafprocedure je schade vergoed te krijgen. Dat is voor slachtoffers een hele mooie gelegenheid om hun schade op een eenvoudige wijze vergoed te krijgen. Maar je ziet dus dat dat zeer belastend is voor het strafproces, omdat de inhoudelijke behandeling dan maar heel beperkt is, maar er heel veel tijd moet worden uitgetrokken voor dat laatste gedeelte. Ik denk dat dat ook een reden is waarom we eigenlijk heel weinig zaken zien terugkomen waarin er echt is vervolgd voor onlinehandelsfraude als we kijken op rechtspraak.nl, maar dat durf ik niet met zekerheid te zeggen.
Wat zou je er nou aan kunnen doen om het strafproces er beter op in te richten? Allereerst zou er kunnen worden geleerd van de ervaringen die zijn opgedaan in het MH17-proces. Daarin was ook sprake van een groot aantal slachtoffers die zich hadden gevoegd als benadeelde partij. Een van de keuzes die daarbij is gemaakt, is om met vaste bedragen te werken. Daardoor is het eenvoudiger om vast te stellen of er schade is geleden door het strafbare feit. Zo ja, dan is dit het vaste bedrag dat in dit geval dan wordt toegekend. Op die manier kan makkelijker door een groot aantal vorderingen heen worden gewerkt en komt er tegelijkertijd een vorm van genoegdoening. Je ziet dat die schadevergoeding en die strafprocedure vooral belangrijk is voor slachtoffers omdat het een zekere mate van genoegdoening aan die slachtoffers geeft; de dader moet hun

die schade dus vergoeden. Op die manier wordt dat tijdens de strafprocedure vereenvoudigd.
Een van de andere dingen die in het kader van de modernisering van de strafvordering nog steeds op de plank ligt en waar nog steeds over nagedacht wordt, is het ontwikkelen van een afzonderlijke procedure waarin het schadevergoedingsproces in de strafprocedure, dus de vordering benadeelde partij, losgekoppeld kan worden van de strafzaak. Zo kan er meer tijd worden vrijgemaakt voor de behandeling van de vorderingen, kan er in de strafprocedure echt alleen worden gefocust op de inhoud van de zaak en kan er vervolgens daarnaast nog tijd worden gemaakt voor de civiele claims. Dat is nog in ontwikkeling, want zoals u weet, is het wetgevingsproces daarvoor nog niet afgelopen en komt dat mogelijk nog in een van de aanvullingswetten terug.

De **voorzitter**:
Dank u wel. Mevrouw Galič.

Mevrouw **Galič**:
Ik ga de tweede vraag voor ons beantwoorden over, zoals u zei, ouderwetse vormen van strafrecht die worden gebruikt om een nieuw fenomeen te bestrijden. Dat fenomeen heeft ook een grensoverschrijdend karakter. Ik ben vrij positief over de bevoegdheden die kunnen worden gebruikt volgens het nieuwe Wetboek van Strafvordering, die eigenlijk ook digitale opsporingsbevoegdheden zijn. Die hebben ook complexe namen, zoals een «netwerkzoeking», maar de politie heeft heel veel kennis en ook vrij veel bevoegdheden om gedigitaliseerd de criminaliteit in bredere zin, dus niet alleen de onlinefraude, op te sporen. Heel veel mogelijkheden bestaan dus al. Ook op het terrein van het grensoverschrijdende karakter van strafbare feiten bestaan er veel mogelijkheden in Europees verband. Ik zal er twee benoemen. Allereerst het Europees onderzoeksbevel. Dat is een richtlijn op Europees niveau op basis waarvan Europese landen samen kunnen werken om een strafbaar feit te vervolgen, eigenlijk. Daarnaast komt nog het al benoemde e-evidencepakket. Dat bestaat uit een richtlijn en een verordening op basis waarvan bijvoorbeeld de Nederlandse politie of justitie internetproviders en andere bedrijven in andere Europese landen kan vragen om gegevens te verstrekken, dus zonder enige inzet van de justitie in dat andere land, en met heel korte deadlines voor de verstrekking van deze persoonsgegevens. Dat is zeker belangrijk en nuttig als het gaat om onlinefraude. Ik denk dus dat de e-Evidenceverordening en ook de richtlijn hiervoor van groot belang zijn.

De **voorzitter**:
Dank u wel. Mevrouw Van 't Hoff-de Goede.

Mevrouw **Van 't Hoff**:
Hartelijk dank. Ik wil eerst even kort ingaan op de laatste vraag, dus waarom de aanpak van daderschap achterblijft bij het grote aantal slachtoffers. De literatuur laat zien dat de meldingsbereidheid onder slachtoffers sowieso ontzettend laag is. Die is nog veel lager dan bij traditionele criminaliteit. Vervolgens is de doorstroom zeer beperkt voor onlinecriminaliteit. Er is in het afgelopen jaar een rapport uitgekomen dat de doorstroom door de strafrechtketen laat zien van een heel groot aantal traditionele zaken versus onlinecriminaliteitszaken. Daarbij zie je dus eigenlijk dat echt een minimaal percentage die keten doorstroomt. Tot slot is de capaciteit van de politie simpelweg niet toereikend voor het enorm toegenomen aantal slachtoffers, zeker als je kijkt naar onlinefraude. Daarbij zou je kunnen overwegen om er fundamenteel anders naar te gaan kijken. Is het wel nodig dat al deze slachtoffers aangifte doen als we ze vervolgens allemaal zes weken later een brief gaan sturen waarin staat dat hun zaak helaas niet opgepakt gaat worden? Welk doel heeft dat dan

precies? Dan zou je dus ook naar een fundamenteel andere aanpak kunnen gaan kijken, waarbij je bijvoorbeeld één meldpunt integreert, waarbij er zeker wel automatisch een aangifte uit rolt, maar waarbij er ook, veel belangrijker, breder melding wordt gedaan, zodat we meer zicht hebben. Daarbij kan ook hulp aan slachtoffers worden verleend. Stel dat je belt en zegt: «Ik heb vijf minuten geleden op een betaallink gedrukt. Ik had dat niet moeten doen. Ik had het niet door, maar zodra ik had betaald wel.» Ik spreek dat soort slachtoffers. Als je dan vijf minuten later jouw bank aan de telefoon hebt, dan kan die mogelijk nog wat. Als je dat soort hulp integreert, dan hebben we uiteindelijk veel meer effect op de zorg voor slachtoffers dan wanneer we alleen de aangiftebereidheid proberen te verhogen.
Dan wilde ik graag nog op uw vraag ingaan over de PNBF. De procedure niet-bancaire fraude verdient inderdaad een andere naam; daar ben ik het helemaal mee eens. Ik doe daar al twee jaar onderzoek naar, dus ik kan daar best wel wat over zeggen. Ik probeer dat heel kort te houden. In het kort hebben we het hier over een afdoening van onlinefraude buiten het strafrecht, waarbij slachtoffers de ontvanger van het geld aansprakelijk kunnen houden. Dat komt eigenlijk heel primair voort uit het feit dat als je zo'n overschrijving doet nadat je een appje hebt gekregen van «hoi, mam», of als je een overschrijving doet in een andere vorm van criminaliteit, we die overschrijving als bewijs hebben. Daarmee kun je dus aantonen wie de ontvanger van het geld is. Volgens het civiel recht in Nederland heb je er gewoon recht op als je zegt: dat had ik niet willen doen; ik wil het graag terug. Dat heeft niks te maken met daders en slachtoffers. In het civiel recht is het een hele andere verhouding tussen de twee partijen. Nu moet je wel weten wie dat is, want je hebt in beginsel alleen een rekeningnummer en een achternaam. De procedure niet-bancaire fraude ziet erop toe dat slachtoffers de naw-gegevens van die ontvanger kunnen opvragen bij hun betaaldienstverlener. Als je die naw-gegevens hebt, kun je bijvoorbeeld naar een deurwaarder. Die gaat dat geld dan voor jou proberen terug te vorderen.
Daar is heel veel over te zeggen; we hebben er inmiddels al heel veel pagina's vol over op papier gezet. Uw vraag is: moeten we niet direct aan alle Nederlanders verkondigen dat dit de manier van werken is? Daar zit zeker iets moois aan, want hoe mooi zou het zijn als elk slachtoffer direct een vordering kan instellen en zijn geld terug kan krijgen? Ik wil echter wijzen op de keerzijde van het hele verhaal, namelijk dat veel van deze begunstigde rekeninghouders geen daders en geen hardcore criminelen zijn. Dit gaat bijvoorbeeld voor een deel om geldezels, die in sommige gevallen gedwongen zijn om mee te werken aan dit delict en in andere gevallen heel kwetsbaar zijn. Dan kun je denken aan lvb, dakloos et cetera. Deze mensen worden zelf via social engineering eigenlijk zover gekregen om hun bankpas af te staan. Vervolgens moeten zij civielrechtelijk het geld terugbetalen en zijn er ook uitspraken van de rechter die zegt: het is hierbij niet relevant dat jij het geld vervolgens hebt afgestaan aan de daadwerkelijke fraudeur; je bent civielrechtelijk aansprakelijk en moet dat terugbetalen. Die keerzijde zijn wij op dit moment aan het optekenen. We hebben daar heel veel onderzoek naar gedaan. In 2026 wil ik heel graag aanbevelingen doen waarbij we beide kanten van de medaille tegelijkertijd kunnen benoemen en niet alleen de voordelen voor potentiële slachtoffers.

De **voorzitter**:
Dank u wel. Er is nog ruimte voor één vraag per persoon als u het kort houdt, en anders niet. Allereerst de heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Dank, voorzitter. Ik heb een vraag aan mevrouw Van 't Hoff-de Goede. Die gaat eigenlijk over uw eerste punt, preventie. Het is best inzichtelijk wat u vertelde, dat ook herhaald slachtofferschap echt een groot risico is. Heeft

u aanbevelingen of suggesties voor hoe je mensen het best weerbaar kan maken tegen dit soort praktijken? Het gaat natuurlijk om een heel grote groep potentiële slachtoffers. Hoe bereik je die, hoe weet je die te vinden en wat zijn bijvoorbeeld goede interventies?

Mevrouw **Michon-Derkzen** (VVD):
Ik zou eigenlijk aan u allen iets willen vragen. Ik weet dat de voorzitter dat niet leuk vindt. We hebben hier als Kamer gezegd dat er een integrale aanpak van onlinefraude moet komen, want je hoort hier al zo veel verschillende dingen en ontwikkelingen. Ik zou willen vragen of u samenwerkt met het ministerie, met een ministerie. Waar vindt u zelf waar het zwaartepunt ligt in de aanpak van onlinefraude, van dit fenomeen? Bent u daar tevreden over? Wat kan volgens u nog worden verbeterd?

Mevrouw **Mutluer** (GroenLinks-PvdA):
Ik denk dat ik de keerzijde die mevrouw Van 't Hoff-de Goede net uitlichtte heel goed snap. Toen ik zelf met deurwaarders meeliep, kwam het voorbeeld van die geldezels ook aan bod. Ik heb ze helaas ook mogen spreken. Ze kunnen geen bankrekening meer openen, hebben onwijs veel schulden. We hebben in een eerder commissiedebat gepleit voor een inkeerregeling. Ik ben benieuwd hoe zij, ook gelet op de aanbevelingen die in 2026 gaan volgen, kijkt naar een inkeerregeling in relatie tot daders die eigenlijk ook slachtoffers zijn, de geldezels.

De **voorzitter**:
We houden het even bij deze drie vragen. Laat ik nu beginnen bij mevrouw Van 't Hoff-de Goede.

Mevrouw **Van 't Hoff**:
Ik begin even met reageren op de vraag hoe we herhaald slachtofferschap kunnen voorkomen. Als ik daar het antwoord op had, was ik daar absoluut mee begonnen. Dat is niet kritisch bedoeld. Het is wel waar we eigenlijk heen willen, dus we hebben echt veel meer onderzoek nodig naar dit thema. Hoe we mensen weerbaar maken tegen onlinecriminaliteit is de hamvraag van ons onderzoeksprogramma. We zijn deze zomer gestart. Ik heb het antwoord dus nog niet. Wat ik wel graag zou willen aanmoedigen, is dat interventies altijd starten met wetenschappers aan boord. Ik ben een praktijkgericht onderzoeker. Ik doe dat niet voor niets aan een hogeschool. Dat heeft ermee te maken dat interventies heel waardevol worden als je start met de kennis die er al is, als je vervolgens onderzoekers laat meedenken over design, zodat het allemaal ook meetbaar wordt, en als je vervolgens gaat evalueren, zodat je echt kunt spreken van een evidence-based interventie. Dat gebeurt gelukkig meer en meer.
Dat haakt ook een beetje aan op de tweede vraag. Zeker als we kijken naar het thema onlinefraude, zien we dat er al integraal wordt samengewerkt door heel veel partijen, onder andere in de werkgroep Integrale aanpak online fraude. Het is dus niet alsof we van nul moeten komen, maar er is veel meer capaciteit en verantwoordelijkheid nodig en veel meer kennis over dit thema voordat we daadwerkelijk stappen kunnen ondernemen. Waar kunnen we dan wel beginnen? Laten we gewoon eens in gesprek gaan met slachtoffers en kijken waardoor ze slachtoffer zijn geworden, waar ze behoefte aan hebben en hoe we ze kunnen helpen, als ze dat willen, om zichzelf beter te beschermen in de toekomst.
En, ten tweede, laten we werken aan social engineering, weerbaarheid tegen social engineering. Want wanneer mensen zich ervan bewust worden dat als ze een appje, een mailtje of wat het ook is krijgen en ze onder druk worden gezet, er ineens heel veel haast bij is en er allemaal dingen van ze worden gevraagd waarvan ze denken «wat is dit eigenlijk», zou je willen dat ze een soort noodknop in hun brein hebben ontwikkeld. Dat is moeilijker gedaan dan gezegd, maar daar moeten we wel met z'n

allen naartoe: neem even een stap terug, denk even na, laat het even liggen, want er is niks wat binnen één minuut gedaan moet worden. Zo kunnen we bijvoorbeeld werken richting weerbaarheid.
Over de integrale aanpak heb ik al even gezegd dat daar dus veel meer capaciteit op het thema en integrale verantwoordelijkheid voor nodig is. Er wordt gewerkt aan een soort stappenplan: waar moet je je als slachtoffer als eerste melden en waar ga je dan daarna naartoe? Het eerste punt – daar zijn die partijen voor zover ik weet samen mee akkoord – moet de betaaldienstverlener zijn, oftewel je bank. Want die kan eerst kijken of er direct kan worden ingegrepen. Als je zo'n betaling tegenhoudt, bevriest of terugstort, dan heb je eigenlijk al heel veel ellende voorkomen die daarna had kunnen komen. Daarna moeten er partijen klaarstaan die dat goed samen oppakken. Dat is ook weer afhankelijk van de voorkeur van slachtoffers, want de een wil wel aangifte doen en de ander niet. Er is dus al het een en ander gebeurd. Er zijn goede stappen gezet, maar er kan nog veel meer. Er zijn hele enthousiaste mensen op dit thema bezig en als zij meer middelen en verantwoordelijkheden krijgen, dan is er denk ik heel veel mogelijk op dit thema.
Dan de laatste vraag. Sorry, ik heb 'm opgeschreven. Die gaat over de inkeerregeling. Ik wil daar niet te lang over uitweiden, want hier begeven we ons op een territorium buiten mijn eigen expertise. Ik vind het wel van cruciaal belang dat geldezels niet als criminelen worden bekeken, maar als slachtoffer/daders. Dat is een complexe groep. We zien dat er heus wel daders tussen zitten, die echt wel weten waar ze aan beginnen, die voor € 50 denken «ik loop toch nul risico» tot ze een brief krijgen of ze even € 4.000 willen terugbetalen die via hun rekening is weggesluisd. Die groep kan je ook anders aanpakken dan de andere groep, die echt risico loopt. Die moeten we helpen om niet verder in de problemen te raken. Dan heb ik het niet alleen over verder in de criminele problemen. Ook als we denken aan schuldenproblematiek, is dat een belangrijk thema om deze vaak jonge kwetsbare groep voor te behoeden.

De **voorzitter**:
Dank u wel. Mevrouw Galič.

Mevrouw **Galič**:
Ik ga me aansluiten bij mevrouw Van 't Hoff-de Goede. Er is heel veel capaciteit nodig voor een integrale aanpak. Waar ligt het zwaartepunt van het probleem volgens mij? Ten eerste is het strafrecht niet de oplossing als het gaat om onlinefraude. Zoals wij al hebben geschreven in ons factsheet, is er een groot belang in de uitwisseling van persoonsgegevens. Dat betekent dus dat heel veel kennis van gegevensbeschermingsrecht nodig is. Deze persoonsgegevens moeten worden uitgewisseld in heel veel gevallen, maar dat moet worden gedaan volgens het gegevensbeschermingsrecht. Dat vind ik belangrijk om te vertellen.

De **voorzitter**:
Dank u wel. Mevrouw Buisman.

Mevrouw **Buisman**:
Even kijken. Ten aanzien van die integrale aanpak van de onlinefraude. Ik heb geen ervaring met samenwerking met verschillende instanties. Wel ben ik op dit moment betrokken bij een groot WODC-onderzoek naar interventies op het terrein van financieel-economische criminaliteit. Dat is een effectstudie daarvan, planevaluatie en procesevaluatie. Wat je daarin terug ziet komen, is dat kennis van elkaars mogelijkheden om in te grijpen, dus kennis van de verschillende interventies die bestaan bij politie en justitie, maar ook bij de ketenpartners, van groot belang is. Ik wees in het kader van onze gespreksnotitie ook al op JUSTIA, dat onder andere door het Openbaar Ministerie en het CCV is ontwikkeld. Daarin zijn al die

verschillende interventies opgenomen en het is doorzoekbaar als je bepaalde dingen wil doen bij een bepaald geval. Ze hebben daar allerlei functies in zitten om op die manier op zoek te kunnen gaan naar de beste oplossing. Dat soort manieren om elkaar te informeren over wat er mogelijk is buiten het strafrecht om of om te bepalen of een zaak nou wel of niet via het strafrecht moet worden afgedaan zijn daarin heel belangrijk. Ik zou graag nog twee punten willen opmerken in het kader van wat mevrouw Van 't Hoff net zei over het voorstel om geen aangifte van slachtoffers te verlangen. Het is belangrijk om je te realiseren dat alleen in het geval van klachtdelicten een aangifte van een slachtoffer wordt vereist om als politie tot opsporing over te gaan. In deze gevallen – ik heb net even gekeken – zie ik niet genoteerd staan dat een klacht vereist is. Dan zou een aantal meldingen voldoende kunnen zijn om te zeggen: we gaan over tot nader onderzoek. Dat zou eventueel ook bij een andere instantie kunnen worden belegd. Daarbij rijst denk ik wel de vraag wat er dan gebeurt met die slachtofferbelangen, want op het op het Openbaar Ministerie rust bijvoorbeeld een plicht om die slachtofferbelangen te waarborgen binnen de strafprocedure. Dat betekent niet alleen het belang bij een mogelijke schadevergoeding, maar bijvoorbeeld ook het recht op informatie en het recht om te spreken. Dus in zoverre kan er dus een vraag rijzen hoe je dan zorgt dat de slachtofferbelangen voldoende worden gewaarborgd. Het kan ook een conclusie zijn dat dit dan in deze gevallen misschien minder noodzakelijk is.
Ten aanzien van de inkeerregeling voor de geldezels is het misschien vruchtbaar om te kijken hoe met slachtoffers van mensenhandel wordt omgegaan. Er zijn namelijk, denk ik, enige gelijkenissen te ontwaren tussen de geldezels en slachtoffers die zowel eerst zijn geronseld als daarna zelf andere slachtoffers ronselen. Daarvoor geldt ook een speciale inkeerregeling.

De **voorzitter**:
Dank u wel. Tot slot mevrouw Junger.

Mevrouw **Junger**:
Heel even over het meervoudige slachtofferschap. Wij doen op de Universiteit Twente in ieder geval al heel erg lang onderzoek naar de vraag hoe je mensen beter kunt informeren. Onze conclusie is dat kennisoverdracht cruciaal is. Dat kan ook zijn hoe je een foute URL in een e-mailadres herkent. Hoe kan je een e-mail begrijpen? Dat kan door te proberen de achtergrond van die e-mail te herkennen. Wij zien ook het volgende. Van de mensen die bijvoorbeeld via e-mail benaderd zijn, zijn degenen die er niet in trappen, in tegenstelling tot degenen die er wel in trappen, degenen die kennis hebben. Zij zeggen bijvoorbeeld «de bank stuurt niet zo'n e-mail» of «ik zag dat dat adres helemaal fout is». Ik denk dus dat kennis heel belangrijk is. Nou is er online, op de website van de bank enzovoort, al heel veel kennis. Het punt is natuurlijk dat mensen die in die e-mail trappen, denken dat het oké is, dus zij gaan niet op zoek naar die kennis. Het is dus belangrijk om die kennis proactief aan ze aan te bieden. Dan is het een beetje lastig dat als je «be aware» tegen ze zegt, ze nog niet meteen weten waar ze op moeten letten. Dan moeten mensen toch het een en ander een beetje gaan bijhouden, bijvoorbeeld dat een bepaalde e-mail de laatste e-mail van de bank is die frauduleus is, of welke technieken de fraudeurs nu toepassen. Dan zul je toch stap voor stap al die opties die er voor fraudeurs bestaan, moeten «adverteren» en mensen ervoor moeten waarschuwen. Ons ideaal was om een online-cursus aan te bieden om mensen te leren hoe je een foute URL herkent. Dat kan door mensen voorbeelden te laten zien en door ze te laten trainen. Dat is niet een one-shot die gaat helpen. Dat moet je blijven doen. Voor ons was het een probleem dat het niet makkelijk is om geld te vinden om die preventieve interventies te gaan ontwikkelen, wat eigenlijk jammer is.

Maar op basis van overzichten van de literatuur en wat we zelf aan onderzoek hebben gedaan, is dit, denk ik, op dit moment de situatie. De vraag bij welk ministerie we dit allemaal moeten gaan onderbrengen, is een leuke vraag. Het dilemma is natuurlijk dat preventie toch het beste is. Wij gaan ervan uit dat er een onuitputtelijke bron van potentiële daders is. Als je op de ene plek een poort afsluit, dan opent zich er weer één op een andere plek. Dan is er ergens weer een beetje activiteit en dan moet je dáár weer ingrijpen. Dat is niet anders. Preventie heeft heel goed geholpen voor de traditionele criminaliteit. Die is tegen de verwachting in op een gegeven moment gestabiliseerd en sinds 2000 afgenomen. Dat was toch voor het belangrijkste deel het resultaat van preventie. Dat zullen we voor onlinefraude ook moeten doen. Dat is voor een deel lastiger. We weten nog niet precies hoe dat moet. We hebben natuurlijk niet alleen daders in Europa, maar ook in Thailand en Cambodja enzovoort. Dan is preventie het slimste. Het lastige is dat als je kijkt wie wat moet doen, dan moeten de banken, bedrijven, de onlinewinkels en de marktplaatsen iets doen en moeten de socialmediaconcerns worden aangepakt. Dat wil je dan een beetje integreren en wie gaat dat dan doen? Een nationaal fraudecentrum. Dat wil je dan ergens onderbrengen. Ik durf het ook niet precies te zeggen.

De **voorzitter**:
Heel hartelijk dank. Nog een hele korte aanvulling van mevrouw Van 't Hoff-de Goede. Dan gaan we daarna verder.

Mevrouw **Van 't Hoff**:
Ik wilde daar inderdaad graag iets aan toevoegen, want ik ben het er helemaal met professor Junger over eens dat als je geen kennis hebt over hoe je je hoort te gedragen, dat gedrag natuurlijk al helemaal niet gaat gebeuren. Maar, zoals ik al zei, we hebben wel meer dan awareness nodig. Maar ik wilde hem ook nog even omdraaien. We leggen hier de verantwoordelijkheid voor eigen veiligheid bij burgers. Het gaat niet alleen om e-mails, want je moet ook je wachtwoord sterk houden, je mag nergens op klikken en je moet al je software updaten. Oftewel, we vragen een breed scala aan gedragingen van burgers en leggen daarvan de verantwoordelijkheid bij de eindgebruiker neer. Met campagnes komen we dan nooit op het punt dat iedereen begrijpt hoe hij zich volledig veilig moet gedragen en dat ook nog eens gaat doen. Moeten we die verantwoordelijkheid dus wel bij de eindgebruiker leggen of moet dat fundamenteel anders worden aangewezen? Dan kun je bijvoorbeeld nadenken over een Outlook dat zich bewust is van de frauduleuze e-mails die verstuurd worden. Met scraping kunnen wij heel makkelijk signaleren dat die e-mails nog steeds worden gekopieerd en naar duizenden en duizenden mensen worden gestuurd. Waarom kan daar niet een geautomatiseerd bericht bij? Zo hoeven mensen niet een nieuwsbrief te lezen over de nieuwste phishingberichten, maar krijgen ze gewoon live, op het moment dat ze hem krijgen, een pop-up: let op, deze is gevlagd als «frauduleus». Dat wilde ik nog even toevoegen.

De **voorzitter**:
Dank u wel. Ik wil u alle vier heel hartelijk bedanken. Het is zeer waardevol om van experts te horen wat hun inzichten zijn. Dank u wel. Dan schors ik voor enkele ogenblikken en vraag ik de volgende gasten om plaats te nemen aan tafel.

De vergadering wordt enkele ogenblikken geschorst.

Blok 2: Publiek/Publiek-private samenwerking

Gesprek met:
- Henriëtte Bongers, directeur-bestuurder Fraudehelpdesk
- Caroline Sander, vertegenwoordiger Electronic Crimes Task Force (ECTF), werkzaam bij de Eenheid Landelijke Opsporing en Interventies van de politie
- Aleid Wolfsen, voorzitter Autoriteit Persoonsgegevens
- Esther Mieremet, projectadviseur bij ECP | Platform voor de Informatie-Samenleving
- Anne Jan Oosterheert, landelijk portefeuillehouder gedigitaliseerde criminaliteit bij de politie

De **voorzitter**:
Welkom terug. We gaan verder met het tweede blok. Dat hebben wij «publiek-private samenwerking» genoemd. Allereerst welkom aan mevrouw Bongers, directeur-bestuurder van de Fraudehelpdesk, mevrouw Sander, vertegenwoordiger van de Electronic Crimes Task Force bij de politie, de heer Wolfsen, voorzitter van de Autoriteit Persoonsgegevens, mevrouw Mieremet, projectadviseur bij ECP, en de heer Oosterheert, landelijk portefeuillehouder gedigitaliseerde criminaliteit bij de politie. Heel goed dat u er allemaal bent. We hebben u gevraagd om een soort pitch of inleiding van een minuut of twee voor te bereiden. Ik weet dat dat lastig is. We zijn niet superstreng, maar we hebben wel kort de tijd. Ik ga u dus vragen om het beknopt te houden, want dan kunnen wij nog met u het gesprek voeren.
Mevrouw Bongers, aan u als eerste het woord.

Mevrouw **Bongers**:
Voorzitter, Kamerleden, dank voor de uitnodiging. Fijn om hier te mogen zijn. Het is ook goed dat het onderwerp onlinefraude op de politieke agenda staat. In de strijd tegen onlinefraude staat de Fraudehelpdesk dagelijks aan de frontlinie als uniek landelijk meldpunt en laagdrempelige vraagbaak waar burgers en ondernemers terecht kunnen met hun vragen, hun zorgen en hun meldingen. Wij bieden persoonlijke hulp, geven mensen handelingsperspectief, wijzen ze de juiste weg en stellen gedupeerden gerust. Zo voorkomen we schade door vroegtijdige signalering en advies. Die meldingen zijn ook goud waard. Ze laten zien wat er in de samenleving gebeurt, vaak nog voordat andere instanties het in beeld hebben.
Onlinefraude is geen randverschijnsel meer. Het is uitgegroeid tot het meest voorkomende delict in Nederland. Een op de vijf Nederlanders is slachtoffer. Dat zijn ongeveer 3 miljoen mensen. Daarnaast krijgt een veel grotere groep te maken met pogingen tot oplichting. De maatschappelijke schade, financieel en emotioneel, is enorm. Wanhoop, schaamte en verlies van vertrouwen in de maatschappij zijn een dagelijkse realiteit voor miljoenen burgers. De urgentie is groot. Dit jaar hebben wij al meer meldingen ontvangen dan in het hele voorgaande jaar. Die trend zet alleen maar door. Vorig jaar ontvingen we 65.000 meldingen en 650.000 valse mails. Op dit moment hebben we al 80.000 meldingen ontvangen. Als deze lijn doorzet, verwachten we binnen vijf jaar 200.000 meldingen. Als ik daar de valse mails bij optel, gaat het om een miljoen mensen die op enig moment in het jaar contact met ons zoeken. Daarbij gaat het niet alleen om phishingmails en telefoonscams, maar ook om complexe vormen van fraude met AI en deepfakes. Fraude treft niet alleen kwetsbare groepen, maar ook digitaal vaardige mensen en ondernemers. Vaak denkt men «het gebeurt mij niet», maar het kan ieder van ons overkomen.
Onze melders willen vooral geholpen worden. Ze willen dat er iets met hun melding gebeurt. Ze voelen zich vaak geen traditioneel slachtoffer,

maar willen wel dat daders worden aangepakt. Wij vervullen een unieke loketfunctie in het bouwen aan maatschappelijke weerbaarheid en dragen bij aan de herkenning van signalen, zodat deze effectiever hun weg weten te vinden naar onder andere de politie. Meldingen worden gestructureerd verzameld, trends worden herkend en informatie wordt geanonimiseerd doorgeleid. Dankzij intensievere samenwerking met de politie en onze andere partners lukt dat steeds beter. Laat ik een voorbeeld geven. We hebben de afgelopen maanden een pilot gedraaid met de politie, waarbij een politiemedewerker is gestationeerd bij de Fraudehelpdesk. Dat leidde tot 40% meer aangiften en veel snellere opvolging. Dat is synergie in de praktijk, en dat is precies wat er nodig is.
Maar we lopen ook tegen grenzen aan. Met een klein team en beperkte middelen verwerken we deze grote aantallen. We hebben al veel bereikt, ook dankzij de politieke steun die we van u hebben gekregen. Denk aan de uitbreiding van onze dienstverlening, de vergroting van onze naamsbekendheid, samenwerking en zichtbaarheid in de media. Wij willen hét nationale loket zijn voor onlinefraude, voor zowel burgers als bedrijven. We willen een plek zijn waar mensen met hun vragen terechtkunnen, waar slachtoffers weten dat ze serieus worden genomen, waar data direct bijdragen aan preventie en opsporing en waar samenwerking in de keten vanzelfsprekend is. Kortom, we zijn er voor de samenleving, dag in, dag uit.
Onze oproep aan u als politiek is: veranker de Fraudehelpdesk structureel als nationaal loket in de aanpak van onlinefraude en ondersteun de duurzame samenwerking met publieke en private partners. Zo laat u zien dat slachtoffers er niet alleen voor staan en dat Nederland klaar is voor een toekomstbestendige aanpak van deze vorm van high-impact crime. Onlinefraude raakt iedereen. De aanpak moet dat ook doen.
Dank u wel.

De **voorzitter**:
Dank u wel. Het woord is aan mevrouw Sander.

Mevrouw **Sander**:
Dank u wel. Hartelijk dank dat ik hier vandaag aanwezig mag zijn. Mijn naam is Caroline Sander en ik zit hier namens de Electronic Crimes Task Force als onderdeel van de Eenheid Landelijke Opsporing, waar dat team onder valt. Ik kom u vandaag vertellen wat de ECTF doet, waar we tegen aanlopen en waar u ons hopelijk bij kan helpen.
De ECTF is een bewezen samenwerking tussen publieke en private partijen, tussen banken, politie en Openbaar Ministerie, die al sinds 2011 digitale bancaire criminaliteit tegengaat, waaronder onlinefraude. Die vereende krachten zijn heel hard nodig in een speelveld dat razendsnel verandert op basis van technologieën die steeds meer vooruitgang boeken. De impact wordt ook steeds groter. Daarom vind ik het ook heel erg belangrijk om hier te zijn vandaag, want de cijfers liegen er niet om. Het is al een paar keer genoemd, maar bijna de helft van het aantal slachtoffers van criminaliteit in 2023 is slachtoffer geworden van een onlinevorm van criminaliteit, waaronder bankhelpdeskfraude, vriend-in-noodfraude en phishing – thema's waar de ECTF aan werkt. Dat is niet zo gek, want geen enkele criminaliteitsvorm is zo schaalbaar en zo toegankelijk als deze vormen van criminaliteit. Om u een voorbeeld te geven: phishingpakketten zijn te koop voor € 150. Daarvoor krijgt u een complete valse bankwebsite en een beheerpanel. De komst van AI en het toenemende aantal datadiefstallen maken dit probleem alleen maar nijpender. Criminelen kunnen steeds gerichter hun werk doen en het aantal criminaliteitsvormen neemt alleen maar toe.
De ECTF is de afgelopen jaren succesvol geweest, maar we moeten niet stilstaan en we moeten ook vooruitkijken. Dat vraagt om anticiperen en slim kunnen opsporen. We hebben vandaag hele mooie voorbeelden

gezien. Ik heb ook positionpapers gelezen waarin preventie centraal staat. Het voorkomen van onlinefraude is enorm belangrijk, want iedere stap die wij kunnen zetten om criminelen te frustreren, is er een richting een veilige samenleving. Maar een stevig sluitstuk is echt net zo belangrijk. Dat vraagt om effectieve opsporing, want alleen zo hebben we echt een impact op het ecosysteem van onlinefraude. Het gaat over de fraudeurs en de criminele netwerken die hierachter zitten. Dat vraagt om samenwerking, brede bestrijding, een offensieve aanpak en meerschaligheid. We hebben het al vaker gehad over het doen van aangifte, maar dat voelt een beetje als dweilen met de kraan open, want één dader maakt niet één slachtoffer, maar wel honderden of soms duizenden slachtoffers. Wij moeten dus onderzoeken draaien die de hele keten aanpakken. Dan gaat het om onderzoek naar money mules, de zogeheten geldezels, maar ook naar de bouwers van dat soort phishingpanels en naar de facilitators, die hele infrastructuren faciliteren om dit soort phishingpanels te beheren. In die opgave, die de ECTF ook heeft, stuiten wij op belemmeringen, namelijk in het delen van data. Signalen komen te laat bij elkaar, waardoor netwerken niet effectief aangepakt kunnen worden, criminelen onder de radar kunnen blijven en er nieuwe slachtoffers blijven vallen. Vandaag vragen wij dan ook eigenlijk aan u om samen met ons en de AP – we hebben ook de positionpaper van Aleid gelezen – te verkennen of wij informatiedeling sneller en effectiever kunnen oppakken. Wellicht kan dat als de ECTF onder de WGS komt te hangen, zodat wij burgers kunnen blijven beschermen en criminelen kunnen oppakken. Uiteraard is het daarbij belangrijk dat de wet- en regelgeving proportioneel is ten aanzien van de privacy, die ook de burger raakt. Daarover zijn wij het volledig met elkaar eens, denk ik. Met een wettelijke verankering hopen wij eigenlijk minder juridische beperkingen te ervaren, waardoor wij effectief kunnen opsporen en echt impact kunnen maken op een vorm van criminaliteit die alleen maar schaalbaarder, sneller en slimmer te werk gaat.
Dank u wel.

De **voorzitter**:
Dank u wel. U noemde hem al, maar nou is het woord aan de heer Wolfsen. Gaat uw gang.

De heer **Wolfsen**:
Dank u wel, meneer de voorzitter en geachte leden. Bedankt voor de uitnodiging om hier met u in gesprek te gaan over onlinefraude. Ik ga mevrouw Sander aan het eind van bijdrage ook wat bedienen, een klein beetje, dus blijft u opletten.
Ook de AP ziet dat het voor mensen in Nederland belangrijk is dat onlinefraude effectiever wordt aangepakt. Ik denk dat we het daar allemaal over eens zijn. In onze gespreksnotitie zijn we ingegaan op hoe dit veilig en met respect voor grondrechten van mensen kan en moet gebeuren. Graag licht ik die punten in deze bijeenkomst nog even toe. Iedereen in Nederland kan te maken krijgen met onlinefraude, zeker als je ziet hoe gedigitaliseerd onze wereld tegenwoordig is. Mensen hebben vaak geen andere keuze dan zaken online te regelen en dat kan grote en ook serieuze risico's met zich meebrengen. De vorige sprekers, de beide buurvrouwen en ook die in het vorige panel, hebben kraakhelder gemaakt hoeveel slachtoffers er worden gemaakt online. In het Actieplan Integrale aanpak online fraude presenteert het kabinet daarom plannen om onlinefraude beter aan te pakken. De AP juicht dit toe, maar bepleit ook dat het zorgvuldig gebeurt en met kraakheldere definities. Dat is essentieel om duidelijk te krijgen wat onlinefraude precies behelst en welke maatregelen daartegen proportioneel, doeltreffend en rechtmatig zijn. Met de uitkomsten van het onderzoek van het Ministerie van Justitie en Veiligheid – dat laten ze nu uitvoeren door TNO – kunnen fraudevormen mogelijk beter worden opgemerkt en dat kan zorgen voor een gerichtere

aanpak van onlinefraude, eventueel met nieuwe wetgeving als mocht blijken uit het onderzoek dat dat nodig is.
De AP stelt dan ook voor dat gekeken wordt naar de mogelijkheden binnen het huidige wettelijke kader, sowieso al, want bestaande wetgeving kan misschien al uitkomst bieden en vaker mogelijkheden bieden dan nu wordt verondersteld. Dat kan ook de aanpak verbeteren. Mocht nieuwe wetgeving nodig zijn om zaken goed of beter te regelen, dan zal de noodzaak daarvan natuurlijk goed moeten worden aangetoond. Dan zal de AP altijd toetsen of dat in verhouding staat tot de inbreuk op de privacyrechten van mensen. Dat is belangrijk voor slachtoffers, maar het is natuurlijk ook belangrijk voor de mensen die verdacht worden of kunnen worden van fraude.
Verder leest de AP in de inbreng van de overige deelnemers meerdere keren dat bij de aanpak van fraude de AVG als een belemmering voor gegevensdeling wordt gezien. Ik benadruk graag dat er juist binnen de AVG veel mogelijkheden zijn om het wel te doen. Vooropstaat dat gegevensdeling natuurlijk altijd rechtmatig moet zijn en gebaseerd moet zijn op een heldere en goede grondslag. Met andere woorden: het delen van informatie kan altijd alleen op basis van – kort samengevat – door u vastgesteld recht. De AP nodigt organisaties en bedrijven die moeite ervaren met de AVG – ook dat komt helaas nog veel voor – graag uit om hierover met ons in gesprek te gaan. De AVG is namelijk niet ingevoerd om het delen van persoonsgegevens te verbieden. Integendeel, zou ik denken. Het moet juist mogelijk zijn om onlinefraude tegen te gaan. Het gaat er wel om dat grondrechten van mensen ook bij het opsporen van fraude worden gerespecteerd, van slachtoffers, maar ook van daders of potentiële verdachten. Als die afweging in de wetgeving en/of de praktijk lastig te maken is – dat kunnen we ons heel goed voorstellen, mevrouw Sander – dan weet u ons te vinden en zullen we helpen waar dat nodig is en kunnen we aanvullend meedenken, of over de juiste uitleg van de wet of over of we moeten bepleiten dat aanvullende wetgeving nodig is.
Tot slot doet de AP ook een beroep op u als leden van de Tweede Kamer. Als wetgever en als controleur kunt u ervoor zorgen dat bij de bestrijding van onlinefraude geen onevenredige inbreuken worden gemaakt op grondrechten. Daarmee kunnen risico's soms zeer vergaand worden afgewend. Zo kunnen we dan voorkomen dat mensen onbedoeld en onterecht worden gediscrimineerd – dat wil zeggen op een discriminatoire wijze worden geselecteerd voor onderzoek; ook dat moeten we samen indringend tegengaan – of dat mensen die nergens van verdacht worden toch intensief worden gevolgd met betrekking tot hun financiële doen en laten. Ook dat moeten we met z'n allen niet willen.
Nogmaals, de AP is graag bereid om daarover in gesprek met iedereen die dat wenst en om iedereen te adviseren die dat wenst. We zien uit naar uw vragen hierover.

De **voorzitter**:
Dank u wel. Dan geef ik het woord aan mevrouw Mieremet.

Mevrouw **Mieremet**:
Dank u wel, voorzitter. Dank voor de uitnodiging. Het is misschien goed om de achtergrond van waarom ik hier zit te duiden. Ik werk bij ECP | Platform voor de InformatieSamenleving. Wij organiseren samenwerkingen, samenwerkingen op het gebied van onder andere waar we hier voor zitten, maar ook op dat van digitalisering in het algemeen. Wij zijn geen expert in de keten, waar u hier wel allerlei experts hoort die een onderdeel daarvan zijn, maar wij zijn ontzettende fan – dat wil ik hier ook graag even melden – van zo'n integrale aanpak. Met elkaar, met private en publieke partijen, samenwerken is de enige manier om dit te doen.
Het doel van dit overleg – ik heb het nog even teruggezocht – is inzicht krijgen in de mogelijke bestrijding van onlinefraude en de mogelijke inzet

van publiek-private samenwerking. Op dat laatste ben ik al kort ingegaan. Wij zijn een pleitbezorger van publiek-private samenwerkingen. Veranker deze samenwerkingen dan ook. Dit project loopt en we merken dat we als het gaat om geld de eindjes weer bij elkaar moeten krijgen om te zorgen dat we straks verder komen. Dit is belangrijk. We zien ook dat de regie en de scope van belang zijn, dus hoe zo'n samenwerking tot stand komt, welke partijen betrokken zijn en hoe ze hun commitment kunnen geven. Straks in de volgende ronde hier zullen partijen daar denk ik ook dingen over vertellen.
Het andere deel is preventie. Daar hebben we hier ook al wat over gehoord. Wat wij zien, is dat er veel fragmentatie ontstaat. Er zijn veel heel goede ideeën en heel veel partijen die samenwerken. Wij zouden in de integrale aanpak graag zien dat daar samenwerking is en dingen beter met elkaar gedeeld worden. Mevrouw Junger sprak bijvoorbeeld net over lesmateriaal. Nou, er is echt heel veel lesmateriaal. We moeten alleen zorgen dat we dat van elkaar kunnen vinden en op de juiste manier kunnen inzetten. Dat vergt dus regie.
Ik denk dat dat even mijn inbreng is tot nu toe. Dank u wel.

De **voorzitter**:
Veel dank. Dan geef ik het woord aan de heer Oosterheert.

De heer **Oosterheert**:
Dank, voorzitter. Dank, commissie. Fijn dat wij uitgenodigd zijn om ons perspectief te geven vanuit de politie. Ik wil u kort mee terug nemen naar de coronatijd. In de coronatijd gebeurde er wat bijzonders. De woninginbraken daalden tot ongeveer nul – dat is ook niet verwonderlijk, want iedereen zat thuis – maar ondertussen zagen wij een enorme stijging in digitale criminaliteit en die stijging is sindsdien niet meer weggegaan. Digitale criminaliteit is sinds dat moment de nummer één criminaliteit van Nederland. We hebben de afgelopen periode veel demonstraties gezien die over diverse onderwerpen gingen, maar er is geen demonstratie voor het aanpakken van onlinecriminaliteit geweest. Dat is best bijzonder, want ontzettend veel Nederlanders zijn hier slachtoffer van en onze aanpak, als de bv Nederland, is nog onvoldoende om hier een antwoord op te vinden. Waar wij in geloven als politie is samenwerking in publiek-private samenwerkingen, zoals met de Fraudehelpdesk en met de ECTF, omdat wij als politie niet het enige antwoord kunnen zijn op deze vormen van criminaliteit. We zullen dus meer barrières moeten opwerpen en daar hebben we dingen in te ontdekken.
Wat hebben we de afgelopen periode wel gedaan? We hebben in de afgelopen tijd gewerkt met de Operatie Centurion. Dat is een operatie vanuit de politie waarin we hebben gekeken of wij veel dichter op deze vormen van criminaliteit kunnen zitten om snel interventies te kunnen doen in het criminele milieu. Dat is relatief succesvol geweest, maar we zijn ook tegen een aantal barrières aangelopen. Eén barrière is bijvoorbeeld de grensoverschrijdendheid. Er is al vaker gesproken, net ook door de wetenschap, over hoe je daarmee omgaat. Ons stelsel is decentraal, ook bij de politie. Dus het lokale gezag bepaalt grotendeels waar onze opsporingscapaciteit aan besteed wordt. U begrijpt dat dat soms ingewikkeld is als het slachtofferschap zich over heel Nederland bevindt en het daderschap ook verspreid is over heel Nederland. Waar doe je dan die zaak naartoe en hoe maak je die keuzes? Het selectiviteitskader speelt daar natuurlijk ook in mee. Bloed aan de muur krijgt altijd meer prioriteit dan onlineslachtofferschap.
Een tweede punt waar we tegenaan liepen is het snel uitwisselen van data. Het uitwisselen van data gaat meestal traag, dat gaat met vorderingen. Daardoor kunnen we niet realtime op deze vormen van criminaliteit zitten. Criminelen zetten soms na een, twee of drie belletjes een telefoon uit, gooien hun simkaart weg en gaan over naar de volgende. Als

wij er niet korter op zitten en samen met de telecomsector barrières gaan opwerpen, zal dit de komende jaren doorgaan zoals het nu gaat en dat betekent dus dat het de nummer één criminaliteit van Nederland zal blijven.
We hebben ook de Digitale Meldkamer geïntroduceerd. Aangejaagd door de wetenschap zeggen we: we moeten slachtofferschap veel meer centraal stellen. Als iemand te maken krijgt met digitale criminaliteit, dan komen we inmiddels met een auto ter plaatse, niet om meteen een dader te pakken, maar wel om het slachtofferschap veel centraler te stellen en om sporen snel veilig te kunnen stellen zodat we kunnen doorpakken. Dat kan ook omdat de traditionele criminaliteit al jaren aan het dalen is.
Doen we al voldoende? Ik denk het niet. Jullie weten, als Kamer, dat de politie financieel onder druk staat. Deze vorm van criminaliteit vraagt om een investering. De investering die nu gedaan wordt, is vrij beperkt. We krijgen er omgerekend ongeveer 4 fte per eenheid bij om deze vormen van criminaliteit aan te pakken. Dat is bijzonder weinig als je kijkt naar de omvang van deze vormen van criminaliteit. Dus is er werk aan de winkel? Ja. Hoe? We doen dit samen met onze ketenpartners door middel van het bestendigen van de Fraudehelpdesk en de samenwerking met de ECTF. Aleid, dat doen we uiteraard in goede samenwerking met de Autoriteit Persoonsgegevens, want we willen staatsrechtelijk blijven handelen.

De **voorzitter**:
Dank u wel. Dan gaan we over tot de vragen. Hiervoor geldt hetzelfde recept. Ik wil eerst de vragen verzamelen. Stelt u vooral korte vragen. Ik ga jullie ook vragen om korte antwoorden te geven, zodat we meerdere vragen kunnen stellen. De heer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Dank voor uw komst en toelichting. Ik heb eerst een vraag aan mevrouw Sander. Toen ik een tijdje geleden bij de politie was, hadden we het over slachtofferschap bij onlinefraude. Toen werd geopperd dat er een framework voor slachtofferpreventie moest komen. Er zijn nog best wat moeilijkheden om personen die potentieel slachtoffer worden of die in veel databases voorkomen, proactief te verwittigen om herhaald slachtofferschap te voorkomen. Zou u kunnen toelichten wat de hobbels op dit moment zijn en wat wel en niet mogelijk is?

Mevrouw **Michon-Derkzen** (VVD):
We hebben het de hele tijd over de aanpak. Ik hoor u allemaal goede dingen zeggen. Het is ook goed dat we het daarover hebben, maar ik hoop dat u elkaar ook ziet zonder dat wij elkaar hier vanmiddag treffen. Ik wil het in dat kader even specifiek hebben over de Fraudehelpdesk, want ik herinner me dat daar een onderzoek naar is geweest. Dat is al even geleden. De politie zegt: we werken samen met de Fraudehelpdesk. Mevrouw Mieremet zegt: het is goed dat er één punt is. Hoe staat het nu met de reactie op dat onderzoek? Misschien is het raar om dit aan u te vragen, maar is de Fraudehelpdesk nu ook hét meldpunt? Want we vinden met z'n allen dat er een meldpunt moet zijn. Of is dat nog steeds een van de openstaande punten bij onlinefraude?

Mevrouw **Mutluer** (GroenLinks-PvdA):
Daar wil ik even op voortborduren. Door de voorgaande sprekers is genoemd dat er een nationaal fraudecentrum moet komen, waar de Fraudehelpdesk eventueel onder kan vallen. Mevrouw Bongers gaf in haar bijdrage aan dat de onlinefraude in een ongekend tempo toeneemt. Mijn vraag is: kunnen jullie dat überhaupt aan, qua mensen, geld, capaciteit en kennis? Want ik weet niet welke taken jullie op dit moment allemaal al uitvoeren. Die zijn volgens mij heel breed. Als we kijken naar het hier en

nu van de Fraudehelpdesk, kunnen jullie het dan aan? Kunnen jullie straks doorgroeien naar een nationaal fraudecentrum en wat is daarvoor nodig?

Mevrouw **Wijen-Nass** (BBB):
Dat was precies ook mijn vraag, maar dat maakt niet uit. Ik stel hier meteen een vervolgvraag over aan mevrouw Bongers. Zij gaf aan dat er ook een rol is weggelegd voor de politiek. Ik vraag mij af: wat verwachten jullie op dit moment exact van de politiek?

De **voorzitter**:
Ik zal hier zelf één vraag aan toevoegen voor de heer Wolfsen. Er is door u en de andere sprekers veel gesproken over gegevensdeling. U zei daarover: ga maar in gesprek met ons; dan kunnen we het erover hebben. Dat klinkt heel verstandig, maar mijn vraag is: kunnen jullie dat waarmaken? Ik heb het dan zowel over de rol – want jullie zijn tegelijkertijd ook de toezichthouder mocht er wat fout gaan – als over de capaciteit. U begrijpt mijn vraag, dus ik hoop dat u die kunt beantwoorden. Misschien kunt u in ieder geval ingaan op de vraag in hoeverre de AP dat ook echt waar kan maken.
Goed. We gaan beginnen met mevrouw Bongers. Volgens mij zijn er drie vragen aan u gesteld.

Mevrouw **Bongers**:
Ik ben nog niet zo ervaren in de Kamer. Ik vergeet de microfoon elke keer. Dank voor de vragen. Er is in 2023 een rapport uitgebracht door het WODC. Daarin is aangegeven dat de Fraudehelpdesk een unieke organisatie is. De taken los van elkaar zijn niet uniek, maar de combinatie wel. Op dit moment is daar nog geen beleidsreactie op verschenen.
Dan de vraag van mevrouw Mutluer over een nationaal fraudecentrum. Wij zijn op dit moment een hele kleine organisatie. We werken met vijftien mensen. Als je kijkt naar wat we allemaal doen, dan zie je dat dat eigenlijk niet in verhouding staat tot de omvang van onze organisatie en de financiering daarvan. We behandelen alle mails en telefoontjes die we binnenkrijgen. Ik gaf net de aantallen aan. Dat geldt ook voor valse e-mails. We zorgen daarnaast voor alerts. We hebben vandaag nog een alert uitgedaan over de Grote Clubactie waarbij kinderen langs de deur komen en je een QR-code moet scannen. Vervolgens blijkt dat je ineens vastzit aan een abonnement. We proberen mensen te waarschuwen met onze alerts. We werken nauw samen met een heel aantal partijen – de politie is net al genoemd – om ervoor te zorgen dat we aan de voorkant informatie verzamelen, zodat de politie en de strafrechtketen verdere stappen kunnen zetten. Er vinden inmiddels ook verkennende gesprekken plaats met de banken.
Maar het vraagt wel heel veel creativiteit van ons om de Fraudehelpdesk in de basis te laten doen waar we voor zijn, namelijk advies geven en helpen. Denk ook aan doorontwikkeling en aan het zo snel mogelijk afdoen van de zorgen van mensen die zich bij ons melden. We willen er ook voor zorgen dat we het makkelijker maken voor mensen om een melding te doen. We zijn bijvoorbeeld bezig met de ontwikkeling van een app. Mensen hebben altijd hun telefoon bij zich, dus dan kunnen ze ook veel makkelijker iets melden. We hebben ook een signaleringsfunctie en we maken trendanalyses. Dat vraagt veel van ons. Eigenlijk is het huidige kader te weinig. Vandaar ook mijn oproep om het te verstevigen. Ik zie ons echt als een soort huisarts. We krijgen heel veel mensen aan de telefoon die nog geen slachtoffer zijn, maar die wel het vertrouwen in de maatschappij verliezen. Ze krijgen bijvoorbeeld een mailtje van de Belastingdienst of van het CJIB en denken: «Is dit nou echt? Waar moet ik op letten? Is dit echt? Help me, Fraudehelpdesk.» We proberen altijd te kijken wat er aan de hand is en we proberen mensen gerust te stellen

door te zeggen: nee, u bent niet gehackt. En als mensen wel benadeeld zijn, dan vertellen we wat het handelingsperspectief is.

De **voorzitter**:
Dank u wel. Mevrouw Sander.

Mevrouw **Sander**:
Als het gaat over slachtofferschap, dan is de ECTF een prachtig voorbeeld. Binnen de ECTF kunnen we modi operandi met elkaar delen. Wat gebeurt er nu? Wat zien banken voorbijkomen als het gaat over de werkwijze van criminelen? Door die informatie met elkaar te delen, kunnen andere banken ook weer maatregelen treffen om hun beveiliging beter op orde te brengen en hun weerbaarheid te vergroten, waardoor we slachtofferschap voorkomen.
Een ander prachtig voorbeeld dat ik mooi vind om te benoemen als het gaat over slachtofferschap, is dat wij onlangs onderzoek hebben gedaan naar wat het met mensen doet als ze slachtoffer zijn van een onlinedelict. Dat is al een paar keer naar voren gekomen. Wat kunnen we met elkaar doen om dat te voorkomen? Die informatie en opbrengsten worden gedeeld binnen de ECTF. Er wordt samen met de banken gekeken hoe we die informatie kunnen terugleggen bij de bankmedewerkers die mensen spreken die potentieel slachtoffer zijn of al slachtoffer zijn geweest. Dat vertaalt zich naar handelingsperspectieven voor bankmedewerkers. Het werd eerder al genoemd: op het moment dat er sprake is van mogelijk slachtofferschap, dan belt een klant als eerste de bank. Wij treffen dat soort maatregelen om hierop te acteren. De ECTF is daar een mooi voorbeeld van.

De **voorzitter**:
Dank u wel. De heer Wolfsen.

De heer **Wolfsen**:
Dank voor de vragen, meneer de voorzitter. Er is inderdaad heel veel gezegd over gegevensdeling. Dat is cruciaal. Als je fraude goed wilt bestrijden, dan moet je persoonsgegevens delen. Daar is ook helemaal niks mis mee, want dat gebeurt voor een uitstekend doel, namelijk het tegengaan van slachtofferschap en criminaliteit. Laat daar geen misverstand over bestaan. Alleen, zoals de heer Oosterheert zo mooi zei: dat moet wel gebeuren binnen de grenzen van de rechtsstaat. Je wilt mensen niet ten onrechte als verdachte aanmerken of ten onrechte controleren. Je wilt data op een nette en rechtmatige manier verzamelen.
Mevrouw Michon-Derkzen vroeg: zien jullie elkaar ook buiten deze zaal? Dat klopt. Een tijdje geleden zaten de heer Oosterheert en mevrouw Bongers in hetzelfde panel als ik bij een door de burgemeester van Apeldoorn georganiseerde bijeenkomst over dit soort problematiek. Daaruit bleek eigenlijk ook dat er een soort – het woord is nog niet gevallen, maar ik noem het maar even – handelingsverlegenheid ontstond, bij politie, private instellingen, banken en onderwijs: wat mag ik delen en wat mag ik niet delen? Toen heb ik ook gezegd dat wij daar veel meer tijd en energie in willen, moeten en kunnen investeren. Voor de ingewikkelde vraagstukken zou het best goed zijn als de Fraudehelpdesk een publiekrechtelijke taak zou krijgen, zeg ik even als pleidooi voor u. Nu is het natuurlijk een private stichting, maar als die een publiekrechtelijke taak zou krijgen, dan kan die veel meer. Als je puur een private instelling bent, dan is dat veel ingewikkelder. Daar wordt enorm veel over getobd. Kunnen we dat waarmaken? Publieke instellingen staan namelijk onder druk; we hebben net de politie in het nieuws gezien en voor ons geldt hetzelfde. We zijn natuurlijk nog steeds best een kleine, kwetsbare organisatie; wel wat groter dan in het verleden, dus we doen wel veel meer op dat vlak.

Ik aarzel even om het te zeggen, maar ik zeg het toch maar, want het is publieke informatie: bij de Belastingdienst is de afgelopen jaren heel veel misgegaan, bijvoorbeeld. Daar was heel veel discussie en heel veel handelingsverlegenheid. Daar werd fraude tegengegaan bij de belastingaangifte; dat wilden ze goed controleren. Wij draaien nu een project met de Belastingdienst, met een klein extra budget, dat op de grote Belastingdienstbegroting een afrondingsverschilletje is. De Belastingdienst is er zeer tevreden over, de Staatssecretaris is er zeer tevreden over en de dg van de Belastingdienst is er zeer tevreden over. Daar helpen we met een dedicated team met vragen als: wat kan er binnen de grenzen van de wet en wat kan er binnen de grenzen van het recht? Dat is zeer behulpzaam voor belastingambtenaren.
Het zou hier eigenlijk ook heel mooi zijn – van tevoren hadden we het er al even over – om een soort dedicated team te hebben dat helpt bij vragen als: wanneer mag het wel, waar is het onduidelijk en waar kunnen wij normuitleg geven? We kunnen dan ook aan u verantwoording afleggen over hoe we dat besteden. Soms lopen we er ook wel tegen aan dat wetgeving dat in de weg staat. We moeten niet meehelpen met het maken van beleid, maar wij kunnen wel zeggen: dit kan niet, maar hier kan de wet vrij simpel worden aangepast. Of we kunnen zeggen wanneer de wetgever aan zet is om de wet aan te passen – tenzij u zegt: dat wil ik niet. Dan is dat ook duidelijk. Maar ik zou daar echt bij kunnen helpen. Als we met zo'n team een aantal jaren werken op gegevensuitdeling binnen de politie, met een klein extra toegespitst budget daarvoor, dan zouden we echt grote stappen vooruit kunnen maken.

De **voorzitter**:
Op persoonlijke titel zeg ik dat er hier aan tafel mooie ideeën ontstaan. Er waren niet direct vragen gesteld aan mevrouw Mieremet en de heer Oosterheert, maar het kan zijn dat u toch ergens op wil reageren, op een vraag of iets wat door de voorgaande sprekers is gezegd. Maar voelt u zich niet verplicht, want we kunnen ook gewoon kijken wat voor nadere vragen er komen. Dat laatste gaan we doen, hoor ik. Ik weet niet of we nog toekomen aan een hele ronde. Het zou wel kunnen; dan zult u een beetje tempo moeten maken, maar dat kunt u. Meneer Six Dijkstra.

De heer **Six Dijkstra** (NSC):
Ik zal snel praten, voorzitter. Ik heb nog een vraag aan mevrouw Sander. Die gaat eigenlijk over wat u zei over de opsporing. Wat wij vaker horen aan deze kant, is dat er bijvoorbeeld bij onlinefraude vaker wordt ingezet op het verstoren dan op het daadwerkelijk opsporen en vervolgen van daders, omdat dat effect mogelijk groter kan zijn. Kunt u ons een beetje meenemen in hoe de afweging daarin wordt gemaakt, of dat effectief is en of dat een middel is dat vaker ingezet zou kunnen worden, om de schade te beperken?

De **voorzitter**:
Mag ik toch mijn eigen voorstel corrigeren en kijken of we toch meteen even kunnen antwoorden? Dan kijken we gewoon hoever we komen. Dat is denk ik slimmer. Kunt u hier meteen op reageren, mevrouw Sander?

Mevrouw **Sander**:
Ja, zeker. Ik denk dat we op allebei moeten inzetten. Als het gaat over het bestrijden van onlinefraude: daarin zit een component die voor een heel groot deel over preventie gaat. Vanuit de politie noemen wij dat ook wel «het tegenhouden» of «het breed bestrijden». Dat gaat dus over andere interventies dan het daadwerkelijk opsporen en vervolgen. Het is allebei belangrijk, want zonder preventie redden we het niet met opsporen, maar zonder opsporen hebben we niets aan preventie. Ik denk dus dat het belangrijk is om op beide in te zetten. Als het gaat om opsporen, is die

meerschaligheid heel erg belangrijk, denk ik. Ik noemde het eerder al. We moeten dus investeren in het aanpakken van de geldezels en de ronselaars, maar we moeten ook zeker kijken naar de grote netwerken die daarachter zitten, die vaak internationaal opereren, en ook naar de facilitators die ervoor zorgen dat dit soort grote phishingcampagnes mogelijk zijn. Het is een combinatie van verschillende manieren van opsporen en bestrijden.
Mijn collega Anne Jan gaf al aan dat we daarbij als politie natuurlijk wel wat te organiseren hebben. Er komt nu 4 fte bij voor de verschillende regio's, maar wat je eigenlijk als politie wil, is dat de aanpak van onlinecriminaliteit daar veel meer in het DNA van het dagelijkse werk komt te zitten. Je zou daar dan met elkaar bijvoorbeeld de onderzoeken rondom de geldezels of de ronselaars kunnen draaien. Dan zou de Eenheid Landelijke Opsporing, waar ik zelf werk, veel meer kunnen zitten op die zware, internationaal georganiseerde netwerken, die hier ook achter zitten, of op die facilitators. Ik denk dus dat die meerschaligheid enorm belangrijk is, samen met de preventieve maatregelen die ook heel hard nodig zijn.

Mevrouw **Michon-Derkzen** (VVD):
Ik wil eigenlijk doorgaan op dat laatste en ik wilde een vraag stellen aan ... Volgens mij de heer Oosterheert? Ik heb slechte ogen. Ik ken de politieorganisatie al een tijdje, maar niet zo goed als u. Ik denk dus dat mevrouw Sander en de Landelijke Eenheid bezig zijn om de grote criminele netwerken en de grote jongens te pakken en interventies te doen op de rest. U heeft het over 4 fte extra per regio. Jullie zullen allemaal zeggen dat 4 fte weinig is, maar wat gebeurt er nou überhaupt in die regio? Is het zo dat die regio vanuit een basisteam ook verticaal omhoog kan tot en met de club van mevrouw Sander en kan vragen: wat moet ik nou doen? Je komt allerlei dingen tegen, er is altijd wat nieuws en als je het snapt, dan is het de volgende dag weer anders, want die criminelen gaan ook allemaal maar weer door. Is het dus zo georganiseerd dat je vanuit basisteams effectiever kan zijn – dat hoop ik dan heel erg – doordat de club van mevrouw Sander daar behulpzaam bij kan zijn? Werkt dat zo? En hoe zou dat kunnen werken?

De heer **Oosterheert**:
Zo werkt het een beetje, maar nog niet in de volle omvang. Met Operatie Centurion hebben we eigenlijk alle data van de aangiftes die binnenkomen op één hoop gegooid, zodat we veel beter in staat zijn om te detecteren welke criminele netwerken hierachter zitten. Even simpel gezegd: we maken daar pakketjes van en die kunnen naar eenheden toe. Die kunnen in de eenheden en ook in het basisteam opgepakt worden, daar waar een van de daders woont. We zijn aan het experimenteren met dat mechanisme, maar dat is verrekte lastig, want deze vorm van criminaliteit moet altijd concurreren met «het bloed aan de muur», de klap-op-de-bekzaak of de woninginbraak. Die selectie van wat we wel doen en wat niet, en hoe we ons moeten verhouden tot deze vormen van criminaliteit, bespreken we zeker met het OM en met onze regioburgemeester. In theorie zou het moeten werken; in de praktijk staan we, in alle eerlijkheid, nog maar aan het begin van deze aanpak en hebben we nog een hele weg te gaan.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Mijn vervolgvraag is dan: hoe kunnen we het versnellen? Waarom stel ik die vraag? Volgens mij hebben we eerder gezegd dat onlinecriminaliteit een high-impact crime is. U zei net dat het de nummer één criminaliteit is in Nederland. Dan is het best gek dat we er nog niet voldoende toe in staat zijn om die te voorkomen of te bestrijden. Ik zou niet willen dat het per eenheid verschilt. Dat is eigenlijk mijn vraag. Als je het wil versnellen,

dan wil je een aanpak hebben waarbij je gegevens met elkaar uit kunt wisselen, waarbij je met de banken werkt en waarbij je met de gemeente en de wijkteams werkt, om de jongeren aan te spreken. Als het een high-impact crime is, dan moet die eenduidige wijze van werken al gereed zijn of jullie team moet daarover nadenken. Doen jullie dat? Hoe gaan we dit in godsnaam versnellen?

De heer **Oosterheert**:
Ik denk dat de structuur om te kunnen gaan versnellen op dit moment gebouwd wordt. Ik kom toch op mijn andere opmerking: het is ook een gezagskwestie. Ons gezag moet dus ook de keuzes maken om hier op in te zetten in de opsporing. Dat is best ingewikkeld. Die meerschaligheid, waar Caroline het net over had, zien wij ontzettend, maar hoe wij het gezag daarop in moeten richten is een zeer complex vraagstuk dat we niet vandaag of morgen hebben opgelost. Ik ben de portefeuillehouder, dus ik zou heel graag een versnelling willen en ik denk ook dat Nederland dat verdient. Maar we hebben echt een aantal taaie vraagstukken te doorbreken. En in alle eerlijkheid: we zijn jarenlang gewend geweest aan fysieke criminaliteit en nu zijn we aan het omturnen naar andere vormen van criminaliteit. Het is ook gewoon een grote mammoettanker, waarbij we stap voor stap moeten ontwikkelen en dingen moeten uitproberen, zoals mevrouw Junger net ook al zei. Als het effectief is, moeten we opschalen en ook zorgen dat het voor de hele politie toepasbaar is. Ik ken de wens dus, en die ondersteun ik ook. Er wordt aan gewerkt, maar ik verwacht niet dat deze morgen af is.

Mevrouw **Sander**:
Ik heb daar een aanvulling op. Dit vraagt om meerdere dingen. Ik heb net in mijn pleidooi al aangegeven dat het een enorm schaalbare vorm van criminaliteit is. Dit is zo schaalbaar dat we daar als politie mee moeten leren omgaan. Dat vraagt dus ook – dat gaf meneer Oosterheert net ook al aan – om het hebben van een soort realtime inzicht in wat hier nu gebeurt. Het gaat hier vooral over vluchtige gegevens, zoals IP-adressen, camerabeelden en de manier waarop die criminelen hun geld van rekening naar rekening naar rekening hoppen. Als wij echt de zaken willen draaien die impact maken – dat is wat je moet als er zo veel slachtoffers zijn – dan moet je dat wel kunnen doen vanuit een goed inzicht in en een scherp beeld van waar we hier mee te maken hebben en wat precies de criminele netwerken zijn die erachter zitten. Laat ik het vergelijken. Bij een woninginbraak ga je naar plaats delict in een woning. Daar vind je allerlei daders en slachtoffers. Dan ga je aan de slag. We hebben hier, bij de ECTF, te maken met heel veel verschillende soorten pd's; dat werd net ook even genoemd. Je hebt een slachtoffer. Bij de banken ligt informatie. Bij de telecombedrijven ligt informatie. Er zijn wellicht ook nog andere partijen bij betrokken. Al die pd's zijn dus noodzakelijk om inzichtelijk te maken waar we hier mee te maken hebben. Die informatie moet wél bij elkaar komen. Daar hebben we echt wat met elkaar op te organiseren.

De **voorzitter**:
Dan stel ik voor het hierbij te laten. Dank u wel, allemaal. Dank u wel, mevrouw Bongers, mevrouw Sander, de heer Wolfsen, mevrouw Mieremet en de heer Oosterheert, voor uw waardevolle inzichten. Wordt vervolgd.

De vergadering wordt enkele ogenblikken geschorst.

Blok 3: Privaat

Gesprek met:
– Paul Nijhof, ad-interimdirecteur Thuiswinkel.org

– Sandra Molenaar, CEO Consumentenbond
– Medy van der Laan, voorzitter Nederlandse Vereniging van Banken

De **voorzitter**:
Welkom terug. Wij gaan weer verder. Hartelijk welkom meneer Nijhof, ad-interimdirecteur van Thuiswinkel.org, mevrouw Molenaar, CEO van de Consumentenbond, en mevrouw Van der Laan, voorzitter van de Nederlandse Vereniging van Banken. Heel goed dat u hier bent. Ik denk dat u net al iets heeft kunnen horen. In ieder geval heeft u ook een positionpaper kunnen inleveren. Er is u gevraagd om ons in twee minuten een inleidend statement mee te geven. Mag ik daarvoor bij u beginnen, meneer Nijhof?

De heer **Nijhof**:
Jazeker. Dank u wel, voorzitter. Dank uiteraard aan uw commissie dat wij hier vandaag mogen zijn om te spreken over onlinefraude. Er is zeker al heel veel over de tafel gegaan en daar zitten ook heel veel goede ideeën en suggesties bij voor verdere samenwerking.
Zoals gezegd, mijn naam is Paul Nijhof en ik ben interim-directeur van Thuiswinkel.org. Wij zijn de brancheorganisatie van de Nederlandse e-commerce. We hebben bijna 2.000 leden en vertegenwoordigen daarmee zo'n 75% van de online retailmarkt en dienstverlening. Dat is een totaalbedrag van 36 miljard euro op jaarbasis qua omzet. U kent ons wellicht van het Thuiswinkel Waarborg, ons keurmerk dat consumenten zekerheid en vertrouwen biedt bij onlineaankopen. Juist dat vertrouwen staat onder druk.
Onlinefraude is de snelst groeiende vorm van criminaliteit. Dat is al eerder aan de orde geweest. In 2024 werden volgens de cijfers die wij hebben kunnen nagaan bij het CBS 2,4 miljoen Nederlanders slachtoffer, met miljarden euro's aan schade. In 80% van de gevallen zien slachtoffers hun geld nooit terug. Voor onze sector is vooral aan- en verkoopfraude de grootste zorg. Bij aankoopfraude is de consument de gedupeerde. Dan kunt u bijvoorbeeld denken aan complete websites die worden nagemaakt met behulp van artificial intelligence, die haast niet meer van echt te onderscheiden zijn. Helaas hebben ook ondernemers last van fraude, waarbij fraudeurs bijvoorbeeld in plaats van een telefoon een steen in retourpakketjes doen of beweren het pakketje nooit te hebben ontvangen. Zowel ondernemers als consumenten zijn dus in groten getale slachtoffer van steeds slimmer wordende criminelen.
Voorzitter. We zijn blij met de integrale aanpak onlinefraude, waar wij ook onderdeel van zijn. Deze heeft partijen dichter bij elkaar gebracht, pilots opgeleverd en kwetsbaarheden zichtbaar gemaakt. Tegelijkertijd staat de aanpak nog wel in de kinderschoenen. Het is nu tijd voor een volwassen aanpak. Het is nu vaak nog te projectmatig en te afhankelijk van vrijwillige inzet. Bestuurlijke regie, structurele financiering en doorzettingsmacht ontbreken. Wat ons betreft kan dat niet meer. De economische en maatschappelijke gevolgen van onlinecriminaliteit vragen om een permanente plek in de criminaliteitsaanpak van het ministerie en de politiek.
Daarbij komt één oplossing telkens terug als het meest kansrijk – daar is al verscheidene malen over gesproken vandaag – en dat is gegevensdeling. We lopen in Nederland echter aan tegen een strenge Autoriteit Persoonsgegevens. In andere landen is er op dat vlak meer mogelijk. Of het wordt als zodanig gepercipieerd, meneer Wolfsen. Dat zou ook kunnen. U had het zelfs over handelingsverlegenheid en dat is ook echt wat wij merken bij marktpartijen. Daarom vragen wij concreet om twee dingen. Eén, een structurele verankering van de integrale aanpak onlinefraude en regie bij het Ministerie van Justitie en Veiligheid met meerjarige financiering en doorzettingsmacht, bijvoorbeeld in de vorm van een taskforce. En twee,

juridische en politieke bevestiging dat gegevensdeling binnen de AVG kan, zodat partijen sneller kunnen ingrijpen.
Voorzitter. De basis is gelegd. Nu is het moment om door te pakken met de regie, juridische helderheid en samenwerking. Daarbij hebben we allemaal een rol te spelen. De Tweede Kamer door politiek urgentie te geven aan dit escalerende probleem. Ook wij hebben een taak om fraude aan te pakken. Zo helpen we onze leden met de juiste interventies en starten wij als Thuiswinkel.org dit jaar een grote consumentencampagne gericht op veilig online shoppen.
Dank u wel.

De **voorzitter**:
U bedankt. Dan geef ik het woord aan mevrouw Molenaar.

Mevrouw **Molenaar**:
Hartelijk dank, voorzitter. Hartelijk dank, commissie. Fijn dat wij vanuit de Consumentenbond een bijdrage mogen leveren vandaag. Ik ben Sandra Molenaar. Als algemeen directeur van de Consumentenbond wil ik natuurlijk allereerst aandacht vragen voor consumenten of burgers die met onlinefraude te maken krijgen. Het is al een paar keer aan de orde geweest. Wie zijn de mensen, vraagt u zich misschien af. Dat zijn wij, dat bent u, dat ben ik. In 2024 – ook dat getal is al een paar keer aan de orde geweest – werd ruim 9% van de bevolking van 15 jaar of ouder slachtoffer van onlineoplichting. Het gaat om 1,4 miljoen mensen. In de afgelopen twaalf maanden had bijna drie vierde van de Nederlanders te maken met een poging tot onlinefraude. Ik hoorde u al even een voorbeeld geven van een appje dat u had ontvangen. Dat is volgens mij een heel bekend voorbeeld, maar er zijn inmiddels elke keer weer nieuwe, andere tactieken.
Bewustwording is natuurlijk van belang. Ik heb ook gehoord dat te veel bewustwording niet altijd helpt. Vanuit de wetenschap is dat net aangegeven. Daar zijn natuurlijk campagnes voor nodig. Wat ook heel belangrijk is, is aandacht voor het taboe rond onlinefraude. Slachtoffers van onlinefraude zijn geneigd om zichzelf de schuld te geven en de omgeving geeft die mensen ook de schuld. Heel veel mensen denken: het overkomt mij niet en andere mensen hebben gewoon niet op zitten letten. Mensen die slachtoffer zijn, zijn slachtoffer van goed voorbereide zware criminaliteit. Jong of oud, hoog- of laagopgeleid, iedereen kan het overkomen. Het gaat om heel gewiekste social engineering, zeker met alle technologische ontwikkelingen die er nu zijn. Het wordt steeds lastiger om echt van onecht te onderscheiden en om je daar als burger of als consument tegen te weren. De schaamte moet eraf. Wat wij ook merken als wij praten met de slachtoffers van fraude, is dat mensen ook een beetje terughoudend worden om zich online te bewegen en het kan toch echt niet de bedoeling zijn dat mensen bijna bang worden om online te bankieren.
Wat wij willen benadrukken is dat wij de motie van u, mevrouw Michon-Derkzen, onderschrijven. Wij zouden graag zien dat de integrale aanpak verder wordt opgeschaald en geprofessionaliseerd. Wij zien graag dat de integrale aanpak echt in een centrale instantie met een eigen bestuur en middelen wordt ondergebracht. Kennis verzamelen is belangrijk, net als kennis delen en snelle interventies coördineren en aansturen. Wat ook nodig is – dat is al een paar keer aan de orde geweest – is één duidelijk centraal meldpunt dat kan zorgen voor de benodigde ondersteuning. Stel daar dan ook voldoende mensen en middelen voor ter beschikking. Ook hierin onderschrijven wij uw motie.
Onze ervaringen met de integrale aanpak onlinefraude zijn echt heel goed, maar we zien wel heel graag dat partijen die nu niet aangesloten zijn zich wel aansluiten. Dan denken wij – ook die partijen zijn al een paar keer aan de orde geweest aan deze tafel – aan de socialmediapartijen en aan de onlinemarkten. Het moet allemaal veel minder vrijblijvend worden.

Tot slot een appel op u. Ik heb begrepen dat morgen de laatste dag is dat de Kamer bijeenkomt voor de verkiezingen. Ik heb hier heel veel eenduidigheid gehoord, dus het zou echt heel mooi zijn als we met al die eensluidende opmerkingen en gelijkluidende wensen toch morgen in de Kamer ook al iets zouden kunnen doen om hier een vervolg aan te geven. Dat is mijn appel aan u.

De **voorzitter**:
Dank u wel. Mevrouw Van der Laan.

Mevrouw **Van der Laan**:
Dank u wel, voorzitter. Bedankt voor de uitnodiging. Heel fijn om hier te zijn, want wij voelen een grote verantwoordelijkheid om te helpen met het tegengaan van onlinefraude. Dat werd ook in het vorige blok al gezegd. Ik sluit me overigens meteen aan bij wat hier is gezegd. Ik het gevoel dat we inderdaad in alle blokken een vrij eensgezind en eenduidig beeld neerzetten en ik sluit me daarbij aan, maar ik leg even een aantal accenten vanuit ons perspectief.
De verschuiving naar onlinecriminaliteit is immens. Daar hebben wij natuurlijk de afgelopen jaren een steeds toenemende taak in gehad en we zijn er ook in toenemende mate slimmer mee omgegaan als bancaire sector. Wij weten steeds beter onze barrières neer te zetten. Wij worden zelf echt ook steeds slimmer in het tegengaan van onlinefraude. De fraudevormen nemen enorm toe, de variatie neemt toe. De bankhelpdeskfraude is een van de bekendere vormen van fraude waar wij ons in het bijzonder mee bezighouden. We hebben – dat is ook belangrijk om even te melden – de afgelopen jaren ongelofelijk geïnvesteerd in het tegengaan van bankhelpdeskfraude. We investeren enorm in bewustwordingscampagnes. Er komt binnenkort weer een nieuwe aan. We zitten in cycli van verschillende bewustwordingscampagnes. Steeds op een andere manier, zodat mensen steeds weer op een ander manier die awareness kunnen inzetten.
We hebben natuurlijk het vieruurstijdslot ingevoerd. Er zijn – dat realiseren mensen zich niet – teams van honderden mensen per bank bezig om verdachte transacties te stoppen, tijdelijk te reserveren, en contact op te nemen met een klant van wie ze denken dat er op dat moment een gesprek mee plaatsvindt. Daarmee houden ze – dat is de schatting van onze banken – op dit moment 80% van de succeskans tegen. Er is dus een belletje en iemand is er bijna, zal ik maar zeggen, en wij houden het dan net, doordat onze banken, onze leden, dan gaan bellen met de klant die aan de lijn zit, tegen. Die criminelen worden steeds slimmer. Die proberen door die vier uur heen te kletsen tegenwoordig. Wij doen er wel wat tegen, maar er zijn mensen die echt zes, zeven uur aan de lijn zitten met een crimineel. We hebben dus ook voor elkaar gekregen dat deze vorm van fraude gehalveerd is. Maar nog steeds voelen we mee, zoals mevrouw Molenaar ook zei: elke fraude is er een te veel. We zijn met name bezorgd over de enorme trauma's die bij mensen ontstaan. Ze slapen er echt maanden niet van. Dat vinden wij heel verschrikkelijk.
Dat betekent ook het volgende. Het is ook in het vorige blok al gezegd. Hoe werken die criminelen? Ze doen het in een veel eerder stadium. Als wij een bankhelpdeskfraude gaan vergoeden via ons coulancekader, is het eigenlijk al te laat, want dan heeft het trauma al plaatsgevonden. Ons pleidooi vandaag is dus om heel erg te kijken naar de stappen daarvóór. Wij doen onze uiterste best. We weten langzamerhand ook niet meer wat we nog meer moeten doen, behalve dat we steeds vaker en steeds sneller weten hoe we die crimineel in zijn volgende stap voor kunnen zijn. Maar het gaat om die stappen daarvóór. Het begint via social media, e-mail en telefoon. Ze proberen alles van je te weten. Ze plaatsen valse advertenties, de hele santenkraam. Onze oproep is dus als volgt. Naast het feit dat we fantastisch samenwerken met alles en iedereen, zeker ook met

telecompartijen, zien we aan de socialmediakant toch dat Nederland voor de grote internationale socialmediaspelers toch slechts een plekje op de wereld is. Het zou echt fijn zijn als ze ook in Nederland interesse zouden tonen, om hier hun taak te vervullen. Het is, denk ik, aan uw Kamer om met ons mee te denken over hoe je dat eventueel een plek zou kunnen geven. Maar er moet ook gedacht worden over hoe je een vorm kan vinden waarin we ze meer verleiden of dwingen – het is maar net hoe je het noemen wil – om aan deze tafel te verschijnen en die rol wat actiever op te pakken. Denk daarbij aan onlineadvertenties beter controleren. In een aantal gevallen zou je kunnen denken aan ID-controles. Er zijn voorbeelden in het buitenland waarbij de ID-controle bij specifieke fraudes leidt tot 85% reductie. Het gaat dan dus om dat type fraude; je kunt er niet alles mee oplossen.
Het is al gezegd: wij steunen de oproep van de politie om de capaciteit goed te houden van harte. We denken echt dat de samenwerking die we nu hebben, ongelofelijk belangrijk is. Alom bekend en door u gesteund, waarvoor dank, is het Line Busy-initiatief. De Minister heeft het overgenomen. Ongelofelijk veel dank daarvoor. Maar eigenlijk is de kern van ons verhaal dat de integrale aanpak superbelangrijk is. Zorg dat justitie het geldt daarvoor blijft houden. Het geld is nu steeds een jaartje vooruit. Het gaat niet over dat wij daar geld van krijgen. Integendeel, het is gewoon het justitiegeld. Wij nemen alle kosten voor eigen rekening. Zorg dus dat het geld om dit aan te pakken, daar blijft stromen. Aan onze samenwerking hoeft u niet zo veel aan te doen: wij werken wel samen.
Het laatste. Dit is in het vorige blok ook al een aantal keer aan de orde geweest. Wat de gegevensdeling betreft steunen wij van harte dat dat op een goeie, zorgvuldige en natuurlijk grondwettelijke manier plaatsvindt. We werken dan graag samen met de AP, maar ook met onze partners, verder uit wat dan precies welke gegevensdeling is.
Over die gegevensdeling gesproken. Dan sluit ik echt af. We hebben het in onze positionpaper het «nationale anti-scamcentrum» genoemd. Je kunt het ook het «nationale fraudecentrum» noemen. Maar de kern is dat wij daar heel graag aan willen bijdragen. We roepen ertoe op om dat te gaan oprichten. Dat zal een publieke instantie worden, dus wij kunnen het niet oprichten. Je hebt namelijk een publieke instantie nodig om bepaalde bevoegdheden te organiseren. Maar ook wij willen er heel graag aan meewerken om dat verder uit te denken. Er wordt nu al aan gewerkt, maar het zou heel fijn zijn als uw Kamer dat initiatief of dat gedachtegoed zou kunnen steunen. Daarmee kun je namelijk alvast praktischere gegevensuitdeling starten en op termijn ook een ongelofelijk sterke samenwerking doorontwikkelen.
Dank je wel.

De **voorzitter**:
Dank u wel. Dan gaan we weer over tot het stellen van de vragen. Laten we gewoon weer beginnen met één vraag per persoon. De genodigden mogen goed opletten aan wie de vraag wordt gericht, want de leden zeggen dat er duidelijk bij.

De heer **Six Dijkstra** (NSC):
Dank voor uw komst. Ik zal niet smokkelen en maar één vraag stellen aan de heer Nijhof. U eindigde uw betoog met het benadrukken van het belang van gegevensdeling. U zei daarbij hobbels te ervaren, ook vanuit het AP. Nou, de heer Wolfsen was hier natuurlijk net. Hij gaf juist aan dat er onder de AVG best veel ruimte is. Hij zei bereid te zijn in gesprek te gaan, om te kijken wat er allemaal mogelijk is. Ik heb dus het idee dat het vooral gaat om juridische onduidelijkheid. Ik ben wel benieuwd of u iets kunt concretiseren. Wat zijn nou dingen waarvan u nu zegt te denken ze op dit moment niet te kunnen, maar die u qua gegevensdeling wel nodig heeft om dit effectief aan te kunnen pakken?

Mevrouw **Michon-Derkzen** (VVD):
Dank aan de sprekers. Ik herken de analyse van mevrouw Molenaar over de schaamte en het grote risico totaal, los van wat er gebeurt met het vertrouwen in jezelf en daarmee in het digitale systeem, waar je ook niet aan kan ontkomen. Ik ben zo benieuwd naar de integrale aanpak. Ik blijf daar maar op doorkauwen. We hebben het namelijk uitgesproken en we vragen ernaar. We krijgen ook elk jaar een brief met de voortgangsrapportage. Ik vraag het omdat u van de private kant komt: met wie heeft u dan contact? Zijn dat Financiën en EZ, de klassieke partners, of is dat ook JenV? Het is vanmiddag een paar keer over zo'n expertisecentrum gegaan. Wat zou u zeggen, is zo'n expertisecentrum van belang voor het uitwisselen van best practices? Of is het van belang om, heel concreet, casuïstiek verder te brengen en meer informatie te kunnen delen met elkaar? Dat hoor ik mevrouw Van der Laan zeggen. Dat is eigenlijk weer een andere vorm van samenwerken. Die vraag zou ik graag aan alle drie de gasten willen stellen.

Mevrouw **Mutluer** (GroenLinks-PvdA):
In het licht van verwachtingsmanagement, wil ik graag het volgende zeggen. We gaan morgen tot een uur of drie in de ochtend in de Kamer blijven, in verband met stemmingen en allerlei tweeminutendebatten. Daar komt dit onderwerp niet in terug. Dat zeg ik meer in het kader van verwachtingsmanagement. Morgen kunnen we dus niks doen, ook niet om drie uur 's nachts! Maar ik zeg u toe dat we dit niet loslaten. Alles wat u heeft gezegd zal, mogelijk na de verkiezingen, door ons verder worden opgepakt. Dat is één.
Dan mijn vraag. Onder andere meneer Nijhof gaf aan dat de integrale aanpak onlinefraude een taskforce moet worden, onder JenV-regie. Er is op dit moment alleen onvoldoende coördinatie en doorzettingsmacht. Iets houdt dit tegen; het lukt maar niet. Dat kan politieke wil zijn of geld; ik heb geen idee. Ik moest het ook heel erg vergelijken met het Nationaal Platform Criminaliteitsbestrijding, waar bedrijven in zitten. Daar lukt het volgens mij iets beter. Wat moet er gebeuren? Wat is nou de belemmering? We gaan er natuurlijk iets aan doen, maar wat kunnen we nog extra en aanvullend doen om dit voor elkaar te krijgen?

Mevrouw **Wijen-Nass** (BBB):
Deze keer geen smokkelvraag van mij. Ik heb een vraag voor mevrouw Van der Laan over het volgende. Ik ben eigenlijk benieuwd hoe het werkt in de praktijk. Heel vaak is het met onlinefraude namelijk zo dat iemand vrijwillig een geldbedrag overmaakt. Is het dan mogelijk om dat geldbedrag nog te laten blokkeren door de bank? Zo ja, binnen welk tijdsbestek? Wat wordt daar door banken nu aan gedaan qua preventie?

De **voorzitter**:
Dank u wel. Ik heb zelf slechts een aanvulling op wat mevrouw Mutluer al heeft gezegd. Morgen komt het thema inderdaad niet zomaar terug, omdat er geen debat is dat hieraan relateert. Maar nog los van de inhoudelijke betrokkenheid die leden hier uitspreken, blijft dit onderwerp ook gewoon op de kennisagenda staan. Een aantal leden keert naar alle waarschijnlijkheid terug. Nou, niks is zeker! Al zijn er ook leden die zeker niet gaan terugkeren. Maar het onderwerp blijft ook op de kennisagenda. De staf is hierin altijd de continue factor, kan ik hier wel verklappen.
Dat gezegd hebbende gaan we over tot het beantwoorden van de vier vragen. Allereerst is het woord aan de heer Nijhof.

De heer **Nijhof**:
Dank u wel. Dan begin ik eerst met de vraag ten aanzien van gegevensdeling en de juridische onduidelijkheid daarover. Wij merken in het gesprek met marktpartijen dat ze heel benauwd zijn om hun vingers te

branden. Zoals wij het zelf zien, zijn er wel degelijk mogelijkheden binnen die wet, maar is er veel onduidelijkheid over wat de consequenties zijn op het moment dat je daarmee aan de gang gaat. Een concreet voorbeeld is dat we binnen de integrale aanpak onlinefraude de intentie hebben slash hadden om proeftuinen op te zetten om te kijken hoe gegevensdeling mogelijk kan worden gemaakt. Uiteindelijk is dat tot nu toe niet voldoende van de grond gekomen, omdat partijen dat niet aandurven. Dat is een initiatief in samenwerking met TNO, maar we krijgen het eigenlijk niet aan het rollen. Is uw vraag daarmee voldoende beantwoord? Ik denk dat het verstandig is – de heer Wolfsen heeft die handreiking ook gedaan – om als sector met de AP in gesprek te gaan. Zo kunnen we kijken wat er wél mogelijk is binnen deze wet- en regelgeving.

De **voorzitter**:
Dank u wel. Mevrouw Molenaar.

Mevrouw **Molenaar**:
Ik reageer dan op de vraag van mevrouw Michon-Derkzen. Zij vroeg wat de ideeën zijn over een meer structurele entiteit die zich bezig gaat houden met de integrale aanpak van onlinefraude. Wij hebben dat natuurlijk niet helemaal uitgewerkt, maar het komt neer op het volgende. Zoals eerder al is gezegd, is er nu een programma waarvan het elke keer onzeker is of er opnieuw geld voor is. Ook de aanwezigheid of medewerking is redelijk vrijblijvend. Dat moet er echt af. We hebben in eerdere sessies gehoord dat het een heel goed idee zou kunnen zijn om de Fraudehelpdesk onderdeel te maken van zo'n nieuw instituut. Daar geloven wij zelf ook in. Wij denken ook dat de Fraudehelpdesk meer kan. Het idee van heel veel loketten komt terug bij meer onderwerpen over hulp aan burgers. Het helpt niet als je mensen heel veel loketten biedt. Het helpt als je één punt biedt waar mensen terechtkunnen om te weten hoe ze de boel moeten blokkeren en waar ze handelingsperspectief krijgen om de schade te beperken.
Ik vond de opmerking van mevrouw Van 't Hoff interessant. Dat herken ik uit mijn privésituatie. Als je aangifte doet en je zes weken later een brief krijgt waarin staat dat er uiteindelijk niks mee wordt gedaan, dan helpt dat mensen niet om aangifte te doen en om het vertrouwen te krijgen dat het wordt opgelost. Dat zijn allemaal onderwerpen die thuishoren bij zo'n nieuw instituut, of hoe je het ook gaat noemen.

De **voorzitter**:
Dank u wel. Mevrouw Van der Laan.

Mevrouw **Van der Laan**:
Dank u wel. Ik kom eerst op de vraag van mevrouw Michon-Derkzen. In aansluiting op wat mevrouw Molenaar aangeeft: we gaan het verder uitwerken, maar de kern van de gedachte is dat als je mensen met een set van bevoegdheden bij elkaar zet, je de effectiviteit enorm kunt vergroten. Met die vorm creëer je ook structureel een publieke plek waar kennis wordt verzameld over deze vorm van fraude, waar die kennis wordt doorontwikkeld en waar alle partijen naartoe kunnen. Ik heb het eigenlijk over een kenniscentrumfunctie. Op termijn willen we ook dat je elkaar ter plekke realtime kunt helpen, maar we moeten nog verder uitwerken hoe je dat zou kunnen doen en welke grondslagen voor gegevensdeling je daarvoor nodig hebt. Dan praat je echt over data-uitwisseling ter plekke.
Ik ga meteen door op de vraag van mevrouw Wijen-Nass. Hoe werkt het in de praktijk? Een klant zit vier à vijf uur aan de lijn. Tegenwoordig is het meestal minimaal vier uur. Er wordt een overboeking gedaan naar een rekening, waarvan de bank een alert krijgt. Daar zitten honderden mensen voor. Er komt een alert binnen. Wat doet de medewerker dan? Die drukt op een knop – bij wijze van spreken, want waarschijnlijk klikt hij of zij iets

aan op het scherm – en zegt: deze betaling houden we even vast. Dan wordt de betaling vastgehouden. De medewerker van de bank belt met de klant. De criminelen die die mensen aan de lijn hebben, zijn getraind op dit proces. Die zeggen van tevoren, in de eerste vier uur, tegen de klant: «Opletten, want het kan zijn dat u gebeld wordt en dan moet u dit zeggen.» Serieus. Ze worden helemaal getraind op dat telefoontje. Dat telefoontje zou onterecht of verkeerd zijn, niet met de goede bedoelingen en noem het allemaal maar op. Ze zeggen: u wordt gebeld en dan moet u dit zeggen.
Ik heb, met een geheimhoudingsverklaring, mogen meeluisteren naar opgeslagen bandjes. Mensen beginnen tijdens die opname te twijfelen. Het betreft gesprekken die met bankmedewerkers plaatsvinden. Andere gesprekken krijg ik niet te horen. Je hoort dat ze zelf al beginnen te twijfelen. Gelukkig gaan ze onze bankmedewerker geloven. Dan ontstaat er een enorme opluchting. Dat is gelukkig op dit moment bij 80% het geval. Maar in 20% van de gevallen komt het voor dat onze bankmedewerker niet wordt geloofd. De crimineel heeft gevraagd om een heel geloofwaardig verhaal neer te zetten, waardoor onze bankmedewerker die mevrouw of meneer begint te geloven. Het komt ook weleens voor dat je belt en het onterecht is, omdat het oprecht een goede overboeking is. Het is voor een bankmedewerker best moeilijk om dat in te schatten, maar zij zijn daar wel zeer, zeer, zeer getraind in. Dan wordt het geblokkeerd, is iedereen opgelucht en is de betaling niet gedaan. Dat is de situatie.
Daarnaast hebben we de preventiekant. Wat betreft de preventie zetten we vol in op campagnes, op de vieruurssituatie. De meeste leden van ons, misschien wel allemaal, hebben waarschuwingen op de startpagina's van hun apps, websites en de hele santenkraam. We zetten vol in op preventie. De awareness kwam nog even aan de orde in het wetenschapsrondje aan het eind. Ik heb het over de kennis en alertheid. Ik heb mijn moeder van 82 ook al op het hart gedrukt hoe ze dit moet aanpakken. Zo doe je dat. Vertel het vooral door. Preventie is voor ons ook echt een hele belangrijke actielijn. Je ziet ook dat dat werkt. Wij testen de campagnes en checken of het doorkomt. Je ziet echt een groeiend bewustzijn, maar je ziet die criminelen daar ook weer meteen op reageren. Dat weet de politie nog veel beter dan wij. Zij verzinnen dan weer wat anders. Het is dus een beetje een race tegen de crimineel.
Wij houden samen met de politie de criminele ontwikkelingen ontzettend goed in de gaten. Hoe ziet die samenwerking eruit? Wij werken samen met de politie en eigenlijk met iedereen. Met wie vindt die samenwerking het minst plaats? De grote internationale socialmediapartijen zijn het moeilijkst om aan tafel te krijgen en om stappen te laten zetten, omdat ze een wereldwijde speler zijn. Het is moeilijk om daar op nationaal niveau tractie op te krijgen. Maar goed, daar pleiten we wel heel erg voor. Dat zou je kunnen organiseren met verplichtingen of andere oplossingen. Je kunt ze ook bij dat centrum betrekken, al is het maar één persoon. Dan zou ik al heel gelukkig zijn. Dat is een beetje het idee. Is dat een voldoende antwoord op de vraag?

De **voorzitter**:
Dat zullen we zo gaan horen. Ik kijk even of er nog vragen zijn. Mevrouw Michon-Derkzen, gaat uw gang.

Mevrouw **Michon-Derkzen** (VVD):
Dank. Ik maak graag van deze gelegenheid gebruik. Ik kijk even naar de heer Nijhof. We hebben het altijd over wat de rol van de organisatie zelf is. De politie moet de criminelen natuurlijk opsporen, maar kun je ook de barrières verhogen? Elke verhoging van een barrière weegt weer op tegen het commerciële belang dat u heeft. Kunt u iets zeggen over hoe de leden van uw organisatie dat afwegen? Een criticaster zou zeggen: er kan misschien nog wel wat meer, maar dat kost geld. Hoe ziet de kosten-

batenanalyse eruit als het gaat om wat je preventief kunt doen? Ik doel op het ophogen van de barrières versus het strijden voor het commerciële belang.

De heer **Nijhof**:
Ik begrijp uw vraag. Het is uiteraard een balancing act. Het begint ermee dat onze leden bestaan bij de gratie van de consument. Wij hebben als sector heel veel belang bij een goede reputatie als het gaat om betrouwbaarheid en veiligheid. Onze leden worden gecertificeerd en op allerlei vlakken langs de meetlat gelegd, waaronder de veiligheid bij onlineaankopen. Wij organiseren, net als hier, rondetafels met onze leden, waarin de grotere en meer geavanceerde leden hun kennis kunnen delen met de kleinere leden. De groten helpen de kleinen. We nodigen ook heel vaak experts uit van buiten onze groep om hun kennis met ons te delen. Maar uiteindelijk is het natuurlijk wel een afweging van de bedrijven zelf hoeveel ze daarin investeren. Maar het commerciële belang om grote problemen te voorkomen is natuurlijk groot.

Mevrouw **Michon-Derkzen** (VVD):
Is dit ooit gekwantificeerd? Heeft u een idee van de schade van onlinefraude voor uw sector?

De heer **Nijhof**:
Dat is ongetwijfeld in kaart gebracht, maar ik heb dat eerlijk gezegd nu niet paraat. Ik hoop dat u mij dat niet kwalijk neemt, maar het is natuurlijk wel een kostenpost voor onze leden.
Ik heb uw vraag volgens mij ook nog niet beantwoord. Ik realiseer me dat ik die nog niet beantwoord heb. U zei: wat is er extra nodig om het beter van de grond te krijgen? Dat hangt samen met de vrijblijvendheid op dit moment. Het is afhankelijk van het initiatief van de partijen zelf. Wij denken echt dat een structurele verankering van die aanpak in een publiek-private taskforce gaat helpen, onder de regie van Justitie en Veiligheid. Wij zien daarin ook een goede link met het Nationaal Platform Criminaliteitsbeheersing, met een juridische borging via de WGS. Als we het veel meer kunnen formaliseren en het een juiste positie kunnen geven in de beeldvorming, dan denken wij dat we echt grote stappen kunnen zetten.

De **voorzitter**:
We waren ook bij u aangekomen voor een volgende vraag, mevrouw Mutluer.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Dank aan de heer Nijhof voor het feit dat hij daarop is teruggekomen.
Ik heb nog een vraag aan mevrouw Van der Laan naar aanleiding van de eerdere vragen die ik stelde over de PNBF-regeling, de regeling waaronder slachtoffers gegevens mogen opvragen. Dat is een interbancaire regeling. Het is geen overheidsregeling. Een van onze verzoeken aan de Minister was: breng dat via een publiekscampagne breed onder de aandacht van velen. Daar is een beetje van afgezien omdat het niet van ons maar van de banken zou zijn. Hoe kijkt u daarnaar? Zou het helpen als daar iets meer aandacht voor zou komen van overheidswege?

Mevrouw **Van der Laan**:
Officieel is dit een verantwoordelijkheid van de Betaalvereniging. Ik kan niet helemaal namens hen spreken. Op zich is dit inderdaad een regeling die bestaat en die ook effectief is in zichzelf, dus als er gebeld wordt of een aanvraag wordt gedaan om naw-gegevens te krijgen. Dan moet die klant uiteindelijk zelf natuurlijk wel op pad met die naw-gegevens om privaatrechtelijk z'n verhaal te halen, dus niet publiek. In die zin begrijpen

wij dus wel dat de overheid wat terughoudend is om hier een rol in te vervullen. De vraag zou dus eigenlijk doorgezet moeten worden naar de Betaalvereniging in hoeverre zij in staat zijn of het wenselijk vinden om hier campagne-achtige dingen in te doen. Het is inderdaad een eigen regeling van de Betaalvereniging. Althans, zij zijn het portaal waarlangs het allemaal gaat. Als er meer aandacht aan moet worden besteed, zou ik echt naar hen gaan. Ik wil de vraag met alle liefde doorgeleiden met het verzoek om uw Kamer erover te informeren of iets anders.

Mevrouw **Mutluer** (GroenLinks-PvdA):
Nee, ik heb zelf contact met ze. Ik was even benieuwd naar uw mening. Want als wij dit een nummer één vorm van criminaliteit vinden ...

Mevrouw **Van der Laan**:
Nou, om het op hele grote schaal te krijgen? Natuurlijk heeft de fraude dan al plaatsgevonden. Het is ook nogal wat. Je geeft wel even de naw-gegevens weg aan iemand en daar wordt wel iets mee gedaan. Om nou te zeggen «iedereen moet dit weten en go, go, go», dat dat de boodschap wordt aan het volk «go, go, go en ga er zelf achteraan»? Want dat is toch eigenlijk waar de voorziening over gaat. Nou ja, ik ga daar geen oordeel over geven, maar als je me vraagt of het de bedoeling is dat we allemaal massaal zelfstandig privaatrechtelijk ons verhaal gaan halen: ja, dat kan. Maar het is eigenlijk meer een vraag voor uw Kamer, hoe belangrijk u het vindt dat mensen daar zelf alsnog extra achteraangaan aan de hand van naw-gegevens. Maar ja, mijn antwoord is: het is aan de Betaalvereniging en, ten tweede, het is best wel iets wat je laat gebeuren. Dus zo.

De **voorzitter**:
Dank. Ik kijk nog één keer naar de kant van de leden. Zijn er nog vragen? Als dat niet het geval is, kijk ik naar uw kant. Zijn er van uw kant nog opmerkingen, nabranders? Dus vragen die niet gesteld zijn, maar die wel een antwoord zouden verdienen? Dat is ook niet het geval.
Dan ga ik ook u heel hartelijk bedanken voor uw bijdrage aan dit rondetafelgesprek. Alle mensen op de publieke tribune ook veel dank voor uw belangstelling. Natuurlijk ook dank aan onze bode, de medewerkers van de Dienst Verslag en Redactie en aan onze griffier. Dank jullie wel allemaal. Zoals gezegd, wordt het thema zeker vervolgd. Het blijft op de kennisagenda staan, maar het is wel aan de Kamer in nieuwe samenstelling.
Ik dank u wel en ik sluit dit rondetafelgesprek.

Sluiting 16.21 uur.