

Gespreksnotitie mr. dr. S.S. Buisman & dr. M. Galič, LL.M.

Rondetafelgesprek online fraude, Vaste Commissie J&V 1 oktober 2025, 14.00 uur

U heeft ons gevraagd om een schriftelijke samenvatting te geven over de mogelijkheden voor bestrijding van online fraude en de inzet van publiek private samenwerkingen bij deze aanpak ter voorbereiding van het rondetafelgesprek met de Vaste Commissie voor Justitie en Veiligheid. Ons standpunt kan als volgt worden samengevat:

1. Er is onvoldoende capaciteit binnen de strafrechtsketen om alle gevallen van onlinefraude via het strafrecht aan te pakken;
2. Daarom is integrale aanpak van online fraude, waarbij onder meer wordt ingezet op preventie en publiek-private samenwerking, van essentieel belang;
3. De inzet van het strafrecht zal om die reden moeten worden beperkt tot de meest ernstige vormen van online fraude (ultimum remedium);
4. Wanneer het strafrecht wordt ingezet dan lijken de huidige opsporingsbevoegdheden afdoende mogelijkheden te bieden;
5. Uitwisseling van persoonsgegevens is in de aanpak van online fraude van belang en is onder voorwaarden ook mogelijk op basis van de AVG.

1. Capaciteit van de strafrechtsketen en omvang onlinefraude

Door de digitalisering van de samenleving zien wij de afgelopen jaren en sterke toename van onlinefraude. In 2024 zijn 1,4 miljoen personen slachtoffer geworden van één of meer vormen van onlinefraude. De gevolgen voor de samenleving zijn groot: financiële, emotionele en psychische schade, en verlies aan vertrouwen in het economische en maatschappelijke verkeer.¹ De strafrechtsketen beschikt echter maar over beperkte capaciteit en is daardoor niet in staat om alle 1,4 gevallen op te pakken. Zo blijkt uit het jaarbericht 2024 van het Openbaar Ministerie dat het in 2024 6.617 zaken op het terrein van gedigitaliseerde criminaliteit heeft afgedaan. Dat is ruim boven de gestelde norm, maar nog steeds niet afdoende om de gehele omvang van het probleem te dekken.² Bovendien is strafrechtelijk ingrijpen slechts reactief: het wordt in beginsel pas ingezet als er al een strafbaar feit is gepleegd. Het is mede om die reden dat in 2022 is ingezet op een integrale aanpak van online fraude.³

2. Belang integrale aanpak online fraude

Met de integrale aanpak van onlinefraude wordt onder meer ingezet op preventie en samenwerking met publieke en private partners om onlinefraude te bestrijden. Bovendien kan onlinefraude via verschillende rechtsgebieden – zoals het privaatrecht, bestuursrecht, tuchtrecht en het strafrecht – worden aangepakt, waardoor verschillende autoriteiten, instanties, instellingen, bedrijven én burgers verantwoordelijk zijn voor het bestrijden van onlinefraude. Dit biedt eveneens een verscheidenheid aan middelen en maatregelen inzake het toezicht op, de opsporing en de afdoening van frauduleuze handelingen.⁴ Denk bijvoorbeeld aan de bestrijding

¹ CBS, 'Online oplichting en fraude', Online Veiligheid en Criminaliteit 2024, 15 april 2025, via www.cbs.nl.

² Openbaar Ministerie, *Jaarbericht 2024*, mei 2025, via www.om.nl.

³ Ministerie van Justitie en Veiligheid, Actieplan 2025. Integrale aanpak online fraude', april 2024, via www.rijksoverheid.nl.

⁴ Ministerie van Justitie en Veiligheid, Actieplan 2025. Integrale aanpak online fraude', april 2024, via www.rijksoverheid.nl.

van aankoopfraude via het Landelijk Meldpunt Internetoplichting en de Fraudehelpdesk, waarbij de focus hoofdzakelijk ligt op verstoringstechnieken om onlinefraude minder aantrekkelijk te maken, zoals het offline halen van frauduleuze webwinkels en advertenties op basis van vrijwillige samenwerking van online platforms en websites. Een dergelijke aanpak heeft ook succes: meer dan 80% van de webshops is binnen 5 dagen uit de lucht. Slechts 12% blijft langer dan 2 weken online.⁵

Een dergelijke aanpak is alleen mogelijk als wordt geïnvesteerd in de samenwerking tussen politie & justitie en publieke en private partners, alsook gegevensuitwisseling tussen deze partijen (zie nader onder 5). Ook is het belangrijk dat de verschillende partners op de hoogte zijn van de mogelijkheden die elk van hen te bieden heeft. In dat kader kan bijvoorbeeld worden gewezen op de JUSTIA-tool van het openbaar ministerie, waarin eenvoudig kan worden gezocht naar mogelijke interventies waarover het OM en externe partners over beschikken voor de aanpak van financieel-economische criminaliteit.⁶

3. Strafrecht als ultimum remedium

De beperkte capaciteit en het reactieve karakter van het strafrecht noopt er ook toe dat keuzes worden gemaakt over welke zaken via het strafrecht dienen te worden afgedaan en welke zaken zich beter lenen voor een alternatieve aanpak. In dat kader zou de inzet van het strafrecht moeten worden beperkt tot de meest ernstige gevallen van online fraude.⁷ Daarbij kan worden gedacht aan gevallen waarbij sprake is van een groot aantal slachtoffers, een hoog schadebedrag, een georganiseerd verband of de complexiteit van het feit vraagt om de inzet van specifieke expertise of strafvorderlijke bevoegdheden.⁸

4. Afdoende mogelijkheden met huidige en toekomstige opsporingsbevoegdheden

Is er sprake van een geval van onlinefraude dat de inzet van het strafrecht rechtvaardigt, dan biedt het huidige Wetboek van Strafvordering al een groot aantal opsporingsbevoegdheden om de daders van de onlinefraude op te sporen. De belangrijkste opsporingsbevoegdheden zijn het vorderen van identificerende en verkeersgegevens, doorzoeking van geautomatiseerde werken, netwerkzoeking tijdens het doorzoeken van plaatsen en aftappen van communicatie. Daarnaast zijn de bevoegdheden inzake het ontoegankelijk maken van gegevens van belang bij de bestrijding van onlinefraude.

Aan deze bevoegdheden worden onder het nieuwe Wetboek van Strafvordering een aantal nieuwe bevoegdheden toegevoegd. Het gaat daarbij om het kennisnemen van gegevens na inbeslagname en de netwerkzoeking na inbeslagname, waarmee reeds ervaring is opgedaan onder de Innovatiewet Strafvordering en waarvan de evaluaties positief zijn. Tevens kunnen het bevel data-analyse door een derde en de stelselmatige locatiebepaling van belang zijn in de opsporing van onlinefraude. De inzet van deze bevoegdheden 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 de bevoegdheden moet goedkeuren.

⁵ Consumentenbond, 'Nepshops: wel betaald, maar niets ontvangen', 24 september 2024, te raadplegen via www.consumentenbond.nl/acties-claims/nieuws/2024/nepshops-betaald-maar-niets-ontvangen.

⁶ CCV, 'Justia-tool gelanceerd voor opsporing en vervolging', 8 april 2024, via www.hetccv.nl.

⁷ Zie in dat verband ook de recente koerswijziging van het Openbaar Ministerie.

⁸ S.S. Buisman, 'Kwalitatieve en transparante fraudebestrijding. Een verkennend onderzoek naar handhavingscriteria voor fraudedelicten', *TBS&H* 2021, nr. 6

Daarmee lijken er afdoende mogelijkheden te bestaan om ernstige gevallen van onlinefraude op te sporen en vervolging zeker te stellen. Kanttekening is daarbij wel dat de aanwezigheid van een grensoverschrijdend aspect de opsporing kan bemoeilijken, nu in die gevallen justitiële samenwerking met het buitenland noodzakelijk is. Dit probleem wordt wel gedeeltelijk aangepakt met de komende e-evidence verordening en richtlijn.

5. Belang van uitwisseling van persoonsgegevens en mogelijkheden daartoe

Zoals hiervoor is aangegeven is in het kader van de integrale aanpak van online fraude de uitwisseling van persoonsgegevens van groot belang.⁹ In dat geval is de Algemene Verordening Gegevensbescherming van toepassing. Dit was niet het onderwerp van onze factsheet, maar verdient onzes inziens niettemin enige aandacht, omdat gegevensbeschermingsrecht soms wordt gezien als een obstakel in de bestrijding van onlinefraude. Dat is echter een misvatting: de AVG staat het uitwisselen van persoonsgegevens voor de bestrijding van onlinefraude toe, mits deze verwerking op een rechtmatige en legitieme manier gebeurt. De verwerking van persoonsgegevens in een mogelijk strafrechtelijke context kan immers aanzienlijke gevolgen hebben voor alle betrokkene personen.

De verwerking van persoonsgegevens, ondanks het bestaan van een gerechtvaardigd belang zoals fraudepreventie, is daarom verbonden aan voorwaarden en beperkingen. De Information Commissioner's Office, de Autoriteit Persoonsgegevens (AP) van het VK,¹⁰ stelt in dat kader onder andere: 'deel alleen persoonsgegevens die echt nodig zijn om het doel te bereiken, neem alle redelijke maatregelen om ervoor te zorgen dat de verwerkte persoonsgegevens niet onjuist of misleidend zijn, en bewaar gedeelde persoonsgegevens niet langer dan nodig is.'¹¹ Er moet daarom specifiek worden aangegeven welk type fraude men probeert te voorkomen en welke gegevens noodzakelijkerwijs moeten worden verwerkt om dat te bereiken. Een algemene verwijzing naar het doel van "fraudebestrijding" in het privacybeleid is derhalve onvoldoende. Verder is het belangrijk om passende technische en organisatorische maatregelen te treffen om gegevens te beveiligen, zowel binnen de eigen organisatie als bij de ontvangende organisatie. Gebrekkige beveiliging leidt regelmatig tot incidenten, wat het belang van zorgvuldige omgang met deze gegevens onderstreept. Tot slot, de rechten van betrokkenen moeten worden gerespecteerd. Bedrijven en andere partijen moeten beschikken over beleid en procedures waarmee mensen gemakkelijk hun rechten op het gebied van gegevensbescherming kunnen uitoefenen. In een overeenkomst voor het delen van gegevens is het daarom goede praktijk om één aanspreekpunt voor mensen aan te wijzen, zodat zij hun rechten zo makkelijk mogelijk kunnen uitoefenen.

⁹ Zie hierover ook de Factsheet Preventie van onlinefraude, lessen uit het buitenland, van collega Marianne Junger.

¹⁰ Information Commissioner's Office, 'Sharing personal information when preventing, detecting and investigating scams and frauds', <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/sharing-personal-information-when-preventing-detecting-and-investigating-scams-and-frauds/>>, geraadpleegd 9 september 2025.

¹¹ Ibid.