Ministerie van Justitie en Veiligheid

Gegevensdeling online fraude

# De AVG is niet het probleem

## Samenvatting Analyse van het huidige kader

Voor private en publieke organisaties en het slachtoffer

Medegefinancierd door de Europese Unie

Integrale aanpak online fraude

# Inleiding

## Waarom deze analyse?

Private en publieke organisaties ervaren belemmeringen in de samenwerking en bij het treffen van interventies omdat het delen van persoonsgegevens over vermeende fraudeurs niet of beperkt is toegestaan. Om een beter beeld te hebben van de juridische kaders is deze analyse opgesteld. Dit document betreft de samenvatting van de analyse, de volledige analyse is online beschikbaar op www.integraleaanpakonlinefraude.nl.[1] Deze analyse geeft een overzicht van de mogelijkheden en onmogelijkheden van gegevensdeling voor 15 private en publieke organisaties en het slachtoffer.

Het CBS rapporteert in de Veiligheidsmonitor[2] dat in 2025 ongeveer 2,5 miljoen mensen van 15 jaar en ouder slachtoffer zijn geweest van online delicten of incidenten. Het vaakst (10 procent) zijn zij het slachtoffer van oplichting, in het bijzonder aankoopfraude en hacken. Bij aankoopfraude worden online gekochte producten of diensten niet geleverd terwijl ze wel betaald zijn. In het geval van hacken breekt iemand met kwade bedoelingen zonder toestemming in op een apparaat (zoals een computer of tablet) of een account (zoals een e-mail- of bankaccount). Meer mensen zijn slachtoffer van het hacken van een account dan van het hacken van een apparaat.

'Online fraude is de snelst groeiende vorm van georganiseerde misdaad' aldus Europol in het recent uitgebrachte rapport 'Internet Organised Crime Threat Assessment (IOCTA) 2026. Er is sprake van een 'velocity gap' tussen de crimineel en de opsporing. Een van de aanbevelingen is om meer samenwerking te faciliteren tussen private en publieke organisaties.

## Het Programma

In het Programma Integrale aanpak online fraude (Programma)[3] werken private en publieke partijen[4] samen om het aantal slachtoffers van online fraude te laten dalen.
Het Programma richt zich op Barrières en interventies, Gegevensdeling, Opvolging door Politie en Openbaar Ministerie, Weerbaarheid van burgers en bedrijven, Hulp aan slachtoffers en Kennis en innovatie.

Private en publieke organisaties die te maken hebben met online fraude moeten zich continu aanpassen aan de professionalisering van de fraudeur zoals een toenemend gebruik van AI om het slachtoffer te misleiden. Voor de crimineel is de instap naar online fraude eenvoudig met 'crime as a service' en de handel in gestolen persoonsgegevens en slachtofferprofielen. Voor de private en publieke organisaties is het een complex vraagstuk met de inzet van artificiële intelligentie, internationale aspecten en diverse wet- en regelgeving. Private en publieke organisaties willen tijdig geinformeerd worden om de juiste interventie te kiezen. Bijvoorbeeld een webshop of vervoerder wil weten of sprake is van een valse e-mail- of afleveradres, een bank of een bankrekeningnummer gebruikt is bij bankhelpdeskfraude. Gegevensdeling en interventies moeten bijdragen aan het voorkomen van online fraude.

1 Publicaties · Integrale aanpak online fraude
2 Veiligheidsmonitor 2025, hoofdstuk 6, CBS, 6. Online criminaliteit | CBS
3 Brief aan de Tweede Kamer, Bestrijding georganiseerde criminaliteit, 29 911, nr. 372, 8 juli 2022, Brief aan de Tweede Kamer, Bestrijding georganiseerde criminaliteit, 29911, 24 februari 2023.
4 Partners van het programma zijn oa. Nederlandse Vereniging van Banken, Thuiswinkel.org, VNO-NCW MKB, Verbond van Verzekeraars, Fraudehelpdesk, Slachtofferhulp Nederland, de Consumentenbond, de VNG, Verbond van Verzekeraars, de Nationale Politie, het Openbaar Ministerie, de ministeries van Economische Zaken, Financiën, Binnenlandse Zaken en Koninkrijksrelaties.

## Belangenafweging

Zonder waarborgen voor de persoon over wie gegevens gedeeld worden, geen gegevensdeling. Het treffen van passende waarborgen bij gegevensverwerking is een wettelijk vereiste. Het ‘onschuld principe’ en ‘niet meerdere keren voor hetzelfde feit veroordeeld worden’ zijn belangrijke principes die gelden in het strafrecht en het strafprocesrecht. Maar hoe werkt de bescherming van een betrokkene als private organisaties persoonsgegevens onderling delen en ieder voor zich maatregelen treft? Tegelijkertijd moeten bedrijven en burgers zich kunnen beschermen tegen digitale criminaliteit. Deze afweging van belangen staat centraal bij gegevensdeling online fraude tussen privaat en publiek en het slachtoffer. Een belangrijke factor in die afweging zijn de getroffen waarborgen.

## Vraagstelling

Op verzoek van de partners van het Programma is in 2025/2026 een analyse uitgevoerd op de huidige kaders van gegevensdeling online fraude.  De volgende vragen zijn leidend geweest:

1. Wat zijn volgens het huidige kader de mogelijkheden en onmogelijkheden in gegevensdeling over online fraude? Het gaat om:
   - Private organisaties zoals banken, betaaldienstverleners, verzekeraars, webshops, vervoerders en telecommunicatie aanbieders;
   - Overige private partijen zoals stichtingen of anti-fraude bedrijven;
   - Publieke organisaties zoals de politie, Rijksdienst voor identiteitsgegevens, de Kamer van Koophandel, de Financiële Inlichtingen Eenheid en gemeenten;
   - Huidige samenwerkingsverbanden;
   - Het slachtoffer.
2. Met welke waarborgen voor een betrokkene over wie gegevens gedeeld worden, moet rekening worden gehouden bij gegevensdeling en welke voorbeelden zijn er in de praktijk te zien?
3. Wat zijn oplossingsrichtingen om tot een zorgvuldige gegevensdeling te komen en wat is hiervoor nodig?

## Wat ging vooraf

Het vraagstuk gegevensdeling en criminaliteitsbestrijding is regelmatig onderwerp van onderzoek geweest waarover de Tweede Kamer is geïnformeerd. In de volledige analyse is een overzicht opgenomen van de belangrijke momenten in de periode van 2007 tot heden.[5]

## Begrippenkader

Online fraude is een containerbegrip waar o.a. bankhelpdeskfraude, hulpvraagfraude, aan- en verkoopfraude en beleggingsfraude onder vallen. Voor deze analyse wordt de volgende definitie gehanteerd:

*Online fraude is bedrog gericht tegen burgers en bedrijven met behulp van een betalingstransactie en met financieel gewin dat niet zonder ICT zou zijn gepleegd.*[6]

Politie en het Openbaar Ministerie (OM) wijzen op de doorontwikkeling van de online fraudevormen. Fraude experts hanteren een meer risicogerichte benadering om online fraudevormen te typeren en bewegen mee met de modus operandi zoals de toepassing van kunstmatige intelligentie.

## Online fraudevormen

Burgers en bedrijven zijn beide het slachtoffer van online fraude. Uit onderzoeken blijkt dat de meeste aangiften geregistreerd worden bij aan- en verkoopfraude en de hoogste schade bij bankhelpdeskfraude en beleggingsfraude.

5 Publicaties · Integrale aanpak online fraude

6 S.S. Buisman, M. Galič, Opsporing en vervolging van onlinefraude onder het huidige en nieuwe wetboek van strafvordering, 16 mei 2025

## Integrale aanpak

In deze analyse wordt gekeken naar gegevensdeling vanuit het perspectief van de integrale aanpak online fraude. Met ‘integrale aanpak’ wordt bedoeld, een samenwerkend geheel tussen private en publieke organisaties volgens afgesproken doelen en kaders.

## Voor wie?

Deze analyse is uitgevoerd voor de private en publieke organisaties die betrokken zijn bij de bestrijding van online fraude en het slachtoffer. Zij krijgen inzicht in wat mogelijk en onmogelijk is in gegevensdeling en waar onduidelijkheden bestaan. Daarnaast is de analyse bedoeld voor beleidsontwikkeling en besluitvorming over de samenwerking in de integrale aanpak en mogelijk aan te passen kaders.

## Actualiteit

Kaders zijn in ontwikkeling zowel op nationaal niveau als op Europees niveau. In deze analyse wordt uitgegaan van de geldende wet- en regelgeving op het moment van schrijven. Waar mogelijk wordt verwezen naar toekomstige regelgeving bijv. vanuit Europa. De analyse zal in ieder geval gedurende het Programma worden geactualiseerd ten behoeve van de besluitvorming over oplossingsrichtingen.

## Scope en aanpak

Voor de analyse is gebruik gemaakt van interviews, onderzoeksrapporten en praktijkcasussen. Voor de inbreng vanuit de praktijk zijn interviews gehouden met oa. privacy- en fraude experts. De casussen hebben betrekking op gegevensdeling tussen private partijen, publieke partijen, binnen samenwerkingsverbanden en het slachtoffer van online fraude. In de reviewronde is de analyse voorgelegd aan oa. de partijen waarop de analyse betrekking heeft.

De analyse bevat op hoofdlijnen uitleg over de fraudevormen en de privacyregels. Het heeft niet de intentie om als handleiding te dienen noch om de noodzaak van gegevensdeling te onderbouwen.

## Vervolgtraject

De derde vraag die voor deze analyse is gesteld: Wat zijn oplossingsrichtingen om tot een zorgvuldige gegevensdeling te komen, komt in het vervolgtraject aan de orde. Parallel aan deze analyse van de juridische kaders wordt op initiatief van het Programma en in opdracht van het ministerie van Justitie en Veiligheid in het kader van kennisopbouw onderzoek gedaan naar de effectiviteit van gegevensdeling en Privacy Enhancing Technologies (PET’s). De uitkomsten van dit onderzoek zullen in de tweede helft van 2026 gebruikt worden om tot oplossingsrichtingen te komen voor de samenwerking tussen de private en publieke partners in de aanpak van online fraude.

# Overzicht

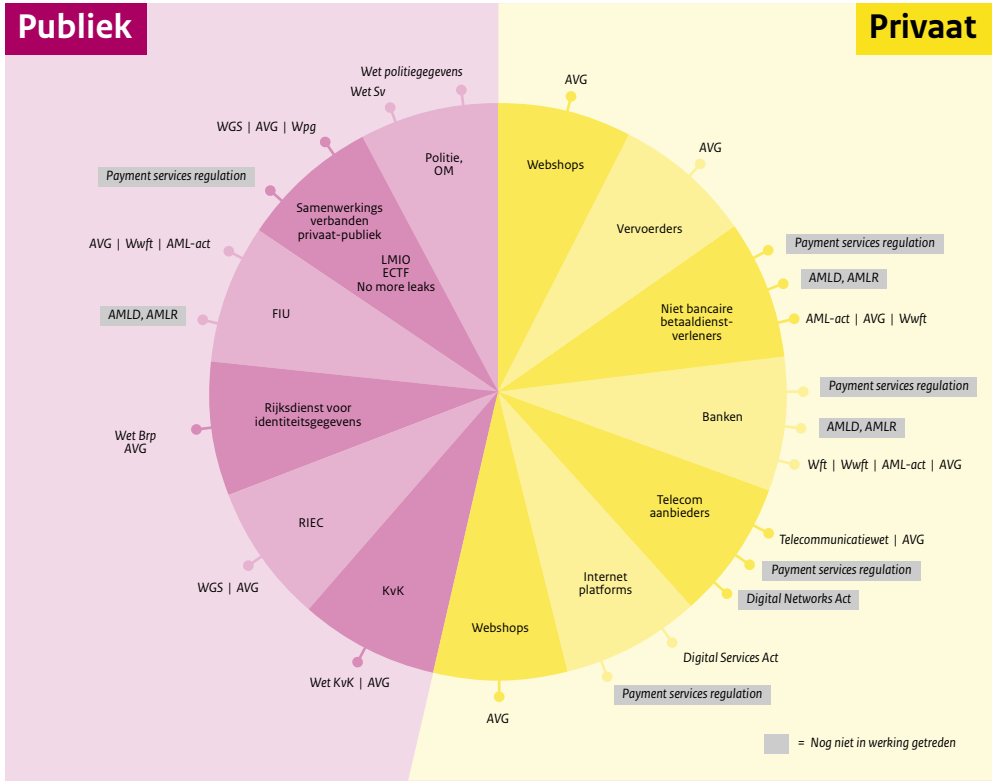
In deze analyse zijn de mogelijkheden en onmogelijkheden in gegevensdeling voor online fraude voor private en publieke partijen en het slachtoffer op een rij gezet. De hoofdconclusies zijn in onderstaande overzichten samengevat.

- Online fraude heeft typisch afwijkende kenmerken ten opzichte van fysieke, traditionele criminaliteit. Uit onderzoeken naar digitale criminaliteit komt het beeld naar voren dat private en publieke organisaties zich richten op preventieve interventies en artificieel intelligence. Zij willen de publiek-private samenwerking in de fraudeketen versterken zowel nationaal als internationaal.

## Typische afwijkende kenmerken van online fraude

- Misleiding van burgers en bedrijven met de inzet van ICT, een betalingstransactie en een verdacht apparaat
- Ongrijpbare verdachten en geldstromen
- Complexe doorontwikkeling van de fraudevormen met AI
- Internationale componenten
- Relatie met hacken, identiteitsdiefstal en witwassen
- Grootschaligheid van slachtoffers
- Lage aangiftebereidheid en victim blaming
- Lage in- en doorstroom in de strafrechtketen
- Diversiteit aan betrokken partijen, rollen, belangen en regelgeving
- Gescheiden informatiebronnen en systemen
- Transitieproces voor de politie organisatie

- Het huidige kader laat een diversiteit zien in nationale en internationale regelgeving voor de private en publieke organisaties die gegevens verwerken over online fraude. Met name wordt de impact van de Europese regelgeving op gegevensdeling voor de financiële sector groot.
- Voor een groot deel van de sectoren is geen sectorale regelgeving die gegevensdeling regelt en zijn de algemene regels van de AVG en de UAVG van toepassing. De AVG geeft meerdere mogelijkheden voor gegevensdeling die op nationaal niveau ingevuld kunnen worden.



- In de EU-regelgeving en op nationaal niveau is een relatie te zien tussen het melden van verdachte transacties van online fraude en de anti-witwasregels.
- Uit de casuïstiek online fraude en de interviews komen verschillende niveaus van gegevensdeling naar voren die gewenst zijn of in de praktijk worden toegepast. Zoals te zien in het kader hiernaast.
- Er zijn in het huidige kader beperkte mogelijkheden voor gegevensdeling. Dit verschilt per sector.
- De vergunningverlening door de Autoriteit Persoonsgegevens (AP) voor het delen van strafrechtelijke persoonsgegevens is sectoraal ingesteld. De financiële en de verzekeringssector hebben een extern verwijsregister met een vergunning van de AP.
- Vrijwel uitgesloten is een vergunning van de AP voor het cross sectoraal delen van persoonsgegevens voor een integrale aanpak. Bij de evaluatie van de UAVG in 2022 wordt de vraag opgeworpen of een vergunningenstelsel het juiste middel is voor gegevensdeling met een grote impact op een betrokkene. Afzonderlijke wetgeving met de nodige waarborgen ligt dan meer voor de hand.
- Andere private sectoren zoals de webshops, PSP en vervoerders beoordelen hun verstrekkingen op grond van de AVG en de UAVG. Omdat er geen sectorale regelgeving is, moeten zij de verstrekking beoordelen op type persoonsgegeven, doel van de verstrekking en de impact op een betrokkene.
- Uit de interviews bleek dat gegevensdeling door private partijen met de politie al dan niet in samenwerkingsverband, in beginsel alleen plaatsvindt via een aangifte of vordering door het Openbaar Ministerie.
- Er zijn meerdere publieke organisaties betrokken bij het tegengaan van online fraude zoals de FIU, de KVK, de politie en de RvIG. Hun taken zijn wettelijk geregeld met weinig tot geen ruimte voor gegevensdeling onderling of met private organisaties.
- De telecommunicatiesector mag op grond van de Telecommunicatiewet verkeersgegevens niet onderling of met derden delen.
- De impact op de betrokkene over wie gegevens gedeeld worden, verschilt eveneens per sector. Bijvoorbeeld het weigeren van een lening heeft een andere impact dan het weigeren van een aankoop.
- De nog in werking te treden Payment Services Regulation (PSR) zal een grote impact op de financiële sector hebben. Fraude incidenten mogen onder voorwaarden rechtstreeks binnen de gehele EU gedeeld worden.

| Opties voor niveaus van gegevensdeling | Kenmerken |
|---|---|
| **Op individueel niveau** | Gegevensverstrekking door en aan het slachtoffer |
| **Op transactieniveau in miniketenverwerking** | Transactie tussen ketenpartners zoals een webshop, PSP en vervoerder. Stopzetten van een verdachte frauduleuze handeling of misbruik van het account van de klant |
| **Sectoraal en cross sectoraal** | Privaat - publieke partijen delen gegevens om elkaar te waarschuwen bijv. via een verwijsregister of op basis van risicoprofielen preventieve interventies te kunnen plegen |
| **Opsporing en vervolging** | Gegevensdeling privaat en publiek voor de opsporing en vervolging |
| **Landelijke alertering online fraude** | Landelijk worden private en publieke partijen en de burger gewaarschuwd |

## Stoplichten model

### Toegestaan in de huidige kaders

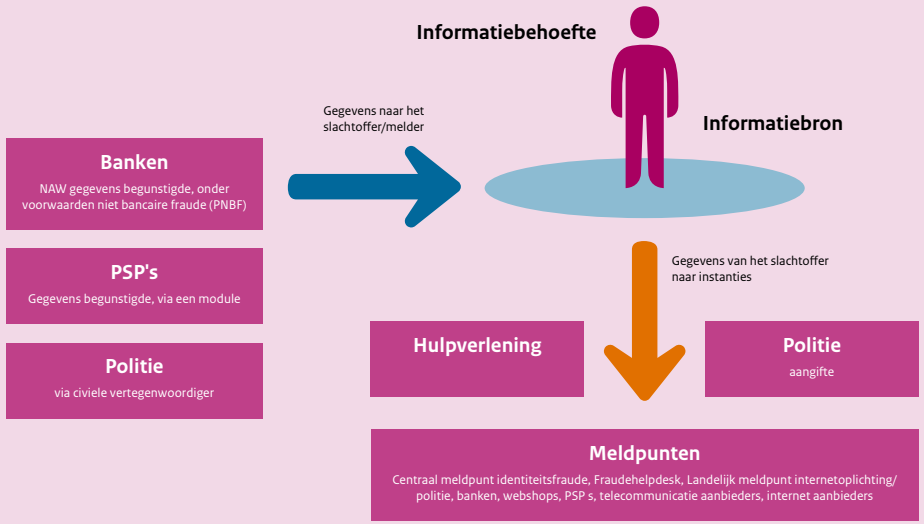
- Modus operandi
- Met vergunning AP een verwijsregister sectoraal
- In mini ketenverband op transactieniveau

### Handelingsverlegenheid

- Van privaat naar politie zonder aangifte, overweging 50 AVG
- Reikwijdte strafrechtelijk persoonsgegeven in de praktijk
- Gegevensdeling in samenwerkingsverbanden politie (ECTF en LMIO)

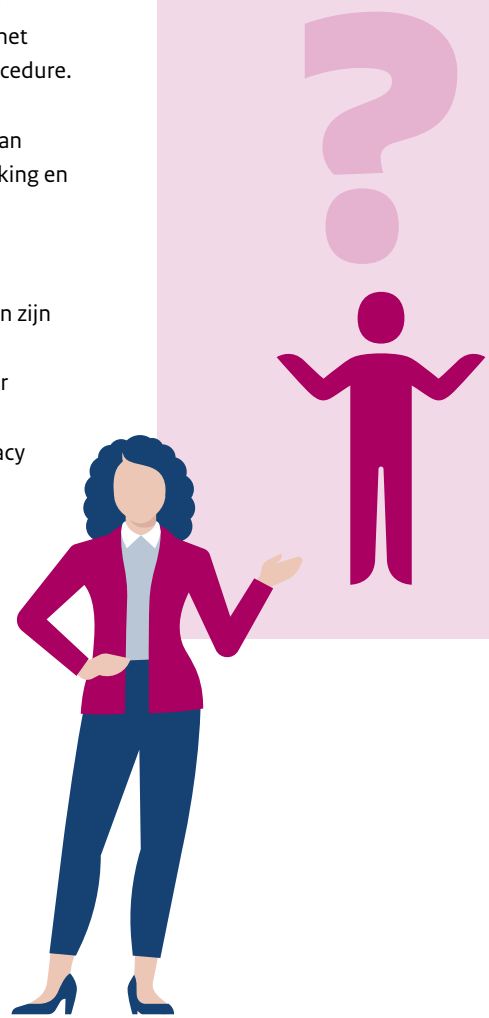
### Niet toegestaan

- Cross sectoraal delen fraude incidenten tussen privaat en publiek
- Cross sectoraal delen om interventies toe te passen
- Uitwisseling fraude incidenten tussen publieke organisaties
- Sandboxing gegevensdeling met PET
- Onderzoek met telecom aanbieders en suspicious devices




- In de PSR is een begin te zien van cross sectorale gegevensdeling tussen betaaldienstverleners, telecommunicatie aanbieders, internetplatforms en advertentiebedrijven.
- Tussen de meldpunten van publieke en private organisaties vindt nagenoeg geen gegevensdeling plaats. Het gaat om gewone en strafrechtelijke persoonsgegevens waarvoor vaak geen grondslag wordt gezien.
- Het slachtoffer van online fraude is een belangrijke bron in de informatieketen maar heeft zelf ook behoefte aan informatie. Bijv. informatie over de te volgen procedure, voortgang van een traject en gegevens om een civiele procedure te starten. Uit de Monitor Identiteit 2025 blijkt dat de meeste slachtoffers zich melden bij de organisatie waar het incident heeft plaatsgevonden zoals een bank of webshop.

- Het slachtoffer bevindt zich in een afhankelijkheidspositie als het gaat om het verkrijgen van gegevens om de schade te verhalen. Het slachtoffer heeft te maken met meerdere routes en mogelijkheden. Gegevensdeling met het slachtoffer hangt af van de organisatie waar het incident heeft plaatsgevonden, de online fraudevorm, het betrokken meldpunt en de procedure. Hiervoor zijn geen wettelijke kaders.
- Naast de beperkte mogelijkheden en onmogelijkheden van gegevensdeling is er sprake van handelingsverlegenheid. Dit belemmert volgens de betrokken organisaties de samenwerking en effectiviteit van de aanpak van online fraude.
- Dit ligt niet aan de AVG maar de praktijk vraagt voor een integrale aanpak om wettelijke grondslagen en ‘guidance’. Dit helpt organisaties in het verantwoord delen van persoonsgegevens mits er een noodzakelijkheid is en de waarborgen voor de betrokkenen zijn ingericht.
- In de praktijk zijn meerdere voorbeelden te vinden van de noodzakelijke waarborgen voor de betrokkene over wie gegevens gedeeld worden. Bijv. geïnformeerd worden over de gegevensdeling, een klachtprocedure tegen onterechte uitsluiting of toepassing van Privacy Enhanced Technology (PET).



## Handelingsverlegenheid heeft betrekking op

- Het vaststellen van een persoonsgegeven en een strafrechtelijk persoonsgegeven in de context van online fraude
- Het structureel verstrekken van strafrechtelijke persoonsgegevens door private partijen aan de politie zonder aangifte of vordering
- Het delen van persoonsgegevens tussen meldpunten
- Het beoordelen van het gerechtvaardigd belang
- Gegevensdeling met het slachtoffer
- Het treffen van passende waarborgen voor de persoon over wie gegevens gedeeld worden

# Hoofdpunten

De hoofdpunten van de analyse van de huidige kaders gegevensdeling online fraude zijn ingedeeld in:

**Online fraude en de huidige kaders** (1 - 3)

**Toepassing van de kaders in de praktijk** (4 - 12)

**Opvallende punten van het huidige kader** (13 - 17)



Deze hoofdpunten worden verder toegelicht in de volledige analyse.[7]

7 Publicaties · Integrale aanpak online fraude

**Online fraude en de huidige kaders**

## 1. Afwijkende kenmerken online fraude

Online fraude heeft andere kenmerken dan een traditioneel strafbaar feit. In het onderzoeksrapport het Fenomeenbeeld Online fraude[8] en het rapport In- en doorstroom in de strafrechtketen (In- en doorstroom) wordt gewezen op:

- de technische complexiteit;
- het massaal slachtofferschap;
- het moeilijk traceren van de verdachte;
- het lastig te bewijzen delict met internationale elementen;
- de doorontwikkeling van de fraudevormen met kunstmatige intelligentie;
- het lage aangifte percentage;
- veel informatie bevindt zich bij private partijen.

De politie geeft aan in transitie te zijn in de aanpak van de traditionele naar de digitale criminaliteit. Uit de in- en doorstroom blijkt dat de meeste zaken niet tot een veroordeling komen bijv. omdat zaken of door de politie of door het OM geseponeerd worden wegens gebrek aan bewijs of een te laag schadebedrag. Uit de gevoerde gesprekken voor deze analyse komt naar voren dat partijen willen inzetten op preventie en het vroegtijdig detecteren van online fraude.

De wetgever heeft bij het wetsartikel over online handelsfraude opgemerkt dat de politie niet alle handelsfraude kan opsporen, de bestrijding is een gedeelde verantwoordelijkheid van zowel private

8 Fenomeenbeeld online fraude 2024, Nationale Politie, https://veiligheidsalliantie.nl/kennisbank/digitale-veiligheid-en-cybercrime/cybercrime-en-gedigitaliseerde-cr/; Rapport In- en doorstroom van online criminaliteit in de strafrechtketen, p. 115, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, in opdracht van het WODC, Amsterdam 2023, In- en doorstroom van online criminaliteit in de strafrechtketen | Rapport | Rijksoverheid.nl

als publieke partijen. Dit is in lijn met de conclusie van Buisman en Galič [9] dat het Wetboek van Strafrecht geen afdoende antwoord is op dit type delict.

Online fraude is geen statische fraudevorm, fraude experts gebruiken geen vaststaande definitie maar bewegen mee met de technologie, de modus operandi en de kenmerken van de fraudevormen zoals het verdachte apparaat. Politie en het OM pleiten voor meer samenwerking tussen private en publieke partijen om tot een brede bestrijding te komen. Het is een andere vorm van criminaliteit waar een andere aanpak nodig is.

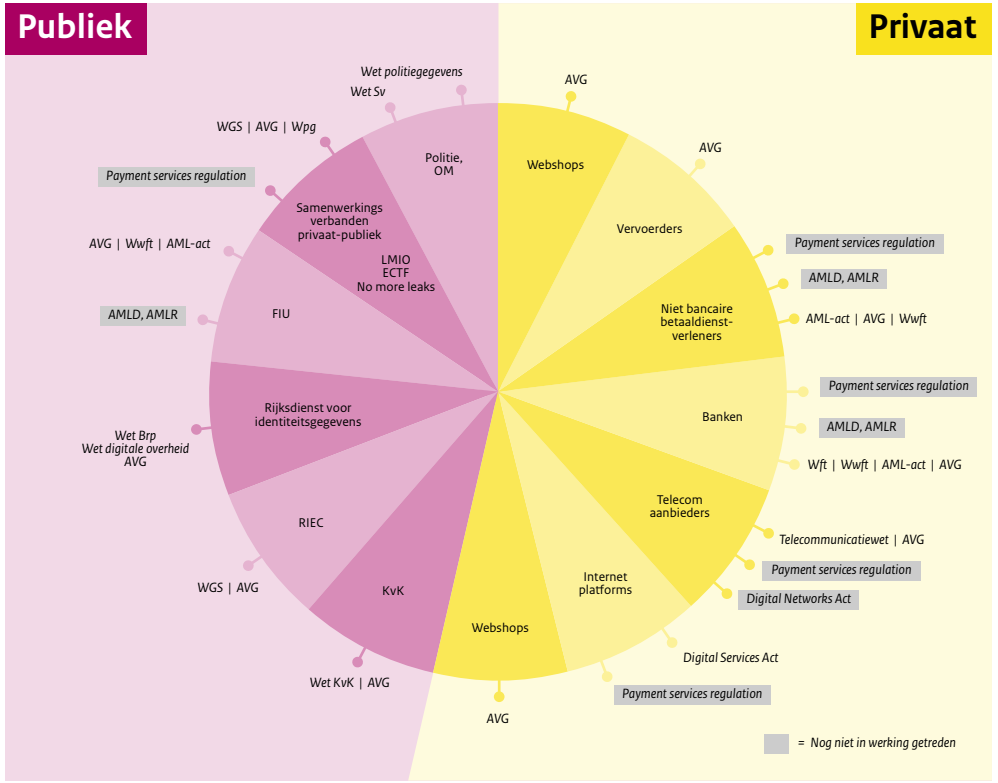
## 2. Verschillende organisaties met verschillende kaders

Voor de analyse van het huidige kader zijn 15 groepen van private en publieke partijen onderscheiden die of slachtoffer zijn en/of bezig zijn online fraude te voorkomen, te detecteren en te bestrijden. Ieder met zijn met eigen wet- en regelgeving, dienstverlening en gegevensverwerkingen. De kaders bestaan uit Europese regelgeving, nationale generieke en sectorale wetgeving, protocollen en convenanten.

Voor gegevensdeling over online fraude in de private sector zijn volgens het huidige kader de AVG en UAVG leidend. De banken en de verzekeraars beschikken nu als enige van de private partijen over een extern verwijsregister waarmee zij binnen hun eigen sector gegevens onderling kunnen delen mits voldaan aan de voorwaarden van een protocol en de verleende vergunning door de Autoriteit Persoonsgegevens (AP).

Voor de andere private partijen zoals de webshops, de vervoerders en de niet-bancaire dienstverleners is er geen sectorale wet, zij vallen terug op de algemene regels van de AVG en de UAVG. Zij beschikken niet over een verwijsregister met een vergunning van de AP.

In de toekomst zullen de Payment Services Regulation en de mogelijke wijziging van de Telecommunicatiewet belangrijke veranderingen tot gevolg hebben. De mogelijkheden voor gegevensdeling over online fraude wordt dan voor bepaalde sectoren uitgebreid. De gevolgen van de Europese regelgeving komen hieronder aan de orde. De minister van Economische Zaken heeft de Tweede Kamer toegezegd met een wetswijziging te komen waarin gegevensdeling door de telecommunicatiesector mogelijk wordt gemaakt.




9 S.S. Buisman, M. Galič, Opsporing en vervolging van onlinefraude onder het huidige en nieuwe wetboek van strafvordering, 16 mei 2025

De publieke partijen die zich bezighouden met online fraudemeldingen en delicten hebben hun eigen sectorale regels en dataverwerking. In de meeste gevallen wordt onderlinge gegevensdeling niet geregeld.

## 3. Internationaal

Online fraude kent geen grenzen en heeft meerdere internationale componenten. Het gaat om buitenlandse bankrekeningnummers, buitenlandse websites, de aanpak van online fraude in andere landen en EU-regelgeving die over datadeling gaan. Voor deze analyse is een quick scan uitgevoerd naar een aantal Europese landen en er is gekeken naar het effect van een aantal EU-richtlijnen en verordeningen.

In de toekomst krijgen de banken en de niet-bancaire financiële dienstverleners (de zgn. payment service providers of betaaldienstverleners) een grondslag om fraude gerelateerde persoonsgegevens te delen in de Payment Services Regulation (PSR).[10] Daarmee worden zij de eerste en tot nu toe de enige groep, die over een grondslag beschikken om persoonsgegevens over betalingsfraude onderling direct te delen. Daarnaast geeft de PSR de betaaldienstverleners de mogelijkheid om met internet serviceproviders, communicatie aanbieders en internetplatforms en advertentiebedrijven gegevens uit te wisselen, art. 59a PSR. Hiermee is de basis gelegd voor toekomstige cross sectorale gegevensdeling over betalingsfraude voor deze categorieën van organisaties.

In het voorstel van de Europese Commissie van de Digitale Networks Act staan aangescherpte verplichtingen voor de aanbieders van elektronische communicatienetwerken of -diensten ter voorkoming en bestrijding van fraude en misbruik. Aanbieders worden verplicht maatregelen te treffen tegen bepaalde online fraude vormen en gegevens uit te wisselen.

10 Provisional agreement resulting from interinstitutional negotiations, subject: Proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010, (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)). Het dossier van het Europees Parlement inzake PSR is hier te vinden.

**Toepassing van het huidige kader in de praktijk**

## 4. Het beoordelen van de verstrekking

De AVG regelt de algemene regels voor de rechtmatigheid van het verwerken van persoonsgegevens. Overweging 47 AVG verwijst naar de grondslag ‘gerechtvaardigd belang’ mits de verwerking strikt gericht is op fraudepreventie. Het belang van een betrokkene (de persoon over wie gegevens verwerkt worden) weegt dan minder zwaar dan het belang van de verwerkingsverantwoordelijke. Hiervoor moet dan wel zijn voldaan aan de voorwaarden van de noodzakelijkheid (nl. de proportionaliteit (niet meer dan nodig) en subsidiariteit (kan het ook anders)), dataminimalisatie en opslagbeperking. Verder moeten geheimhoudingsplichten kunnen worden doorbroken.
Zonder ‘guidance’ of sectorale wetgeving zijn deze beoordelingen niet eenvoudig toe te passen en afhankelijk van de omstandigheden zoals het verband tussen de doeleinden van de verschillende verwerkingen, de verhouding met de betrokkene, de aard van de gegevens, de mogelijke gevolgen voor de betrokkene en de getroffen waarborgen.
Uit de casuïstiek en gehouden interviews komen meerdere doelen voor gegevensdeling naar voren. Het gaat om:

- de uitvoering van een wettelijke taak
- de opsporing en vervolging van strafbare feiten
- het doen van onderzoek naar een incident
- het toepassen van interventies preventief en reactief
- ondersteunen en beschermen van het slachtoffer
- het leveren van een dienst op grond van een overeenkomst
- internationale samenwerking.

## 5. Gegevensdeling binnen en tussen private partijen

Er zijn in het huidige kader beperkte mogelijkheden voor gegevensdeling. Per sector is dit verschillend ingekleurd. De vergunningverlening door de Autoriteit Persoonsgegevens (AP) voor het delen van strafrechtelijke persoonsgegevens is sectoraal ingesteld. De financiële en de verzekeringssector hebben een extern verwijsregister met een vergunning van de AP. Vrijwel uitgesloten is een vergunning van de AP voor het cross sectoraal delen van persoonsgegevens voor een integrale aanpak.

De impact op de betrokkene over wie gegevens gedeeld worden, verschilt eveneens per sector. Bijv. het weigeren van een lening heeft een andere impact dan het weigeren van een aankoop.

Een grote impact op de financiële sector zal de nog in werking te treden Payment Service Regulation (PSR) hebben. Fraude incidenten mogen dan onder voorwaarden rechtstreeks binnen de gehele EU gedeeld worden. In de PSR is een begin te zien van cross sectorale gegevensdeling tussen betaaldienstverleners, telecommunicatie aanbieders, internetplatforms en advertentiebedrijven. Voor de telecommunicatie aanbieders is voor het delen van verkeersgegevens ook een aanpassing in de Telecommunicatiewet nodig.

Bij een aantal online fraudevormen is een mogelijkheid om gewone persoonsgegevens te delen als sprake is van een transactie strikt ter preventie en mits voldaan is aan de voorwaarden van het gerechtvaardigd belang of ter uitvoering van een overeenkomst met de betrokkene. Dit is ter beoordeling van de individuele organisatie. Hierbij kan de praktijk ondersteund worden met bijv. een handreiking of protocol voor de sector. Voor alle fraudevormen geldt dat cross sectoraal delen van databestanden niet is toegestaan. Wel kunnen de modus operandi sectoraal en cross sectoraal worden gedeeld.
Onderstaand overzicht laat de huidige mogelijkheden van gegevensdeling per fraudevorm zien ingedeeld naar sectoraal, in mini ketenverband en cross sectoraal.

| Fraudevorm | Mogelijk te delen | | | Niet mogelijk te delen |
|---|---|---|---|---|
| | Sectoraal | Mini keten: transactie | Cross sectoraal | |
| **Bankhelpdesk-fraude** | Banken kunnen strafrechtelijke persoonsgegevens onderling delen via het extern verwijsregister met vergunning AP volgens het PIFI | Gewone persoonsgegevens met de telecom mits gerechtvaardigd belang, gericht op een transactie. | alleen modus operandi | Banken kunnen geen strafrechtelijke persoonsgegevens zonder hit in het EVR met elkaar delen, noch met andere private organisaties. Telecom mag geen verkeersgegevens delen. |
| **Verkoopfraude** Slachtoffer webshops, of klant met gehackt account | | Gewone persoonsgegevens gericht op een transactie ogv overeenkomst of gerechtvaardigd belang | alleen modus operandi | Webshops kunnen geen strafrechtelijke persoonsgegevens met elkaar delen noch met andere private organisaties. |
| **Aankoopfraude** Consument het slachtoffer | Banken kunnen gewone persoonsgegevens delen om een transactie te blokkeren, mits ger. belang en passende waarborgen. | | alleen modus operandi | Banken kunnen geen strafrechtelijke persoonsgegevens zonder hit in het EVR met elkaar delen, noch met andere private organisaties. |
| **Vriend-in-noodfraude** | Banken kunnen gewone persoonsgegevens delen om een transactie te blokkeren, mits ger. belang en passende waarborgen. | Gewone persoonsgegevens met de telecom gericht op een transactie mits gerechtvaardigd belang | alleen modus operandi | Telecom, banken, platforms kunnen geen strafrechtelijke persoonsgegevens met elkaar delen. |
| **Beleggingsfraude** | Beleggingsmaatschappijen kunnen gewone persoonsgegevens delen om een transactie te blokkeren, mits ger. belang en passende waarborgen. | Gewone persoonsgegevens gericht op een transactie ogv overeenkomst. | alleen modus operandi | Beleggingsmij. kunnen geen strafrechtelijke persoonsgegevens met elkaar noch met andere private organisaties. |
| **Verzekeringsfraude** | Verzekeraars kunnen strafrechtelijke persoonsgegevens onderling delen via EVR met vergunning AP | | alleen modus operandi | Verzekeraars kunnen geen strafrechtelijke persoonsgegevens zonder hit in het EVR met elkaar delen, noch met andere private organisaties. |
| **Identiteitsfraude** | | Gewone persoonsgegevens gericht op een transactie ogv overeenkomst. | alleen modus operandi | Private en publieke organisaties kunnen geen strafrechtelijke persoonsgegevens met elkaar delen. |

## 6. Gegevensdeling met de politie

**Gegevensverstrekking door de politie**
Op grond van de Wpg kan de politie politiegegevens verstrekken aan private partijen onder voorwaarden. Het gaat om structureel volgens het Besluit politiegegevens, op incidentele basis en in een samenwerkingsverband (18, 19 en 20 Wpg). Uit de gesprekken met experts en de casuïstiek blijken de meeste vragen te zijn aan de kant van de organisaties die gegevens willen verstrekken aan de politie.

**Gegevensverstrekking aan de politie**
Er zijn bij de politie op landelijk en eenheidsniveau meerdere samenwerkingsverbanden met private organisaties voor verschillende fraudevormen. Meest bekende zijn het Landelijk meldpunt internetoplichting (LMIO), het Electronic crime taskforce (ECTF) en No more leaks. De set van gegevens die onderling gedeeld wordt, staat in de regeling van het samenwerkingsverband. Een samenwerkingsverband op grond van de Wpg geeft de private partijen geen grondslag om gegevens te verstrekken.

Bij de gegevensdeling met de politie, al dan niet in een samenwerkingsverband, valt op dat private partijen in beginsel geen persoonsgegevens aan de politie verstrekken tenzij sprake is van een aangifte of vordering door het Openbaar Ministerie[11]. Private organisaties zien geen grondslag voor gegevensdeling met de politie behalve via het doen van aangifte of een vordering door het OM. Hierdoor komt de gegevensdeling met de politie bijv. in de aanloop van de aangifte niet op gang. Dit heeft oa. tot gevolg dat in de onderzoeksfase in de aanloop naar de aangifte geen gegevens gedeeld worden met de politie. Er is in dit stadium van het lopende onderzoek nog onvoldoende informatie om tot een aangifte of vordering over te gaan. Hierdoor worden tijdens het onderzoek voorafgaand aan de aangifte geen verbanden gelegd om netwerken van fraudeurs te detecteren en te betrekken in het opsporingsonderzoek. Volgens de private en publieke partijen in een samenwerkingsverband belemmert de aangifte of vordering als enige middel, het functioneren van de samenwerking. Hiermee worden de doelstellingen van het samenwerkingsverband minder goed bereikt.

In overweging 50 AVG staat een verwijzing naar het ‘aanwijzen van mogelijke strafbare feiten door de verwerkingsverantwoordelijke aan een bevoegde instantie moet worden beschouwd als een gerechtvaardigd belang van de verwerkingsverantwoordelijke’. Hieruit blijkt dat het de bedoeling is dat persoonsgegevens met de politie kunnen worden gedeeld. In de praktijk bestaan verschillende interpretaties van deze overweging. Het kan opgevat worden als een grondslag voor de verwerking inclusief de verstrekking van gewone en strafrechtelijke persoonsgegevens aan de politie. Vanuit de praktijk is behoefte aan duidelijkheid hierover. Guidance is nodig van bijv. de AP.

In het nieuwe wetboek van Strafvordering worden nieuwe digitale bevoegdheden opgenomen. Deze geven een aantal digitale handvaten voor het OM en politie om online fraude aan te pakken. Dit zou een oplossing kunnen zijn om met behulp van de data-analyses door private partijen, online fraude aan te pakken, onder de conditie van het bevel van het OM. Het is aan de politie en het OM en private partners om te beoordelen of deze nieuwe bevoegdheden voldoende zijn om de beperkingen in gegevensdeling op te lossen.

## 7. Samenwerkingsverbanden

In het huidige kader kan gegevensdeling plaatsvinden binnen een samenwerkingsverband. Een samenwerkingsverband kan op verschillende manieren tot stand komen. Partijen kunnen zelf een samenwerkingsverband vormen, de politie kan een samenwerkingsverband inrichten op grond van de Wpg en er zijn samenwerkingsverbanden op grond van een wet zoals de Wet gegevensverwerking door samenwerkingsverbanden (WGS).

Voor online fraude bestaan nu alleen samenwerkingsverbanden van de politie met derden op grond van de art. 20 Wpg.
Een samenwerkingsverband geeft als zodanig geen grondslag om gegevens te delen. De samenwerkingsverbanden Electronic crimes taskforce (ECTF) en het Landelijk meldpunt Internet Oplichting, ervaren knelpunten in de gegevensdeling met de private partners. Zoals toegelicht onder punt 6.

11 Art. 126nd Wetboek van Strafvordering

Samenwerkingsverbanden in de WGS zoals het Financieel Expertise Centrum (FEC) is een privaat-publiek samenwerkingsverband dat zich richt op het versterken van de integriteit van het financiële stelsel bijv. door het terugdringen van criminele geldstromen. De informatie-uitwisseling gebeurt in de taskforces: de Serious Crime Taskforce en de Taskforce Terrorismefinanciering. Oplichting behoorde in 2025 volgens het jaarverslag van het FEC tot de top 3 van risico's van de ontvangen signalen door het FEC-informatie platform.

## 8. Rijksdienst voor identiteitsgegevens

De RvIG heeft een sleutelpositie in het stelsel van identiteitsgegevens. Het heeft stelselverantwoordelijkheden en vervult beheerstaken. De RvIG werkt aan het optimaliseren van het uitreiken van identiteitsbewijzen en de betrouwbaarheid daarvan, zorgt voor de registratie van meldingen over identiteitsfraude en helpt de melder om de ID-fraude te stoppen door met andere instanties gegevens te delen en voert landelijke taken uit voor de basisregistratie personen bij gemeenten. Naast de rol als beheerder heeft de RvIG te maken met strafbare feiten waarvoor het samenwerkt met oa. politie, de Koninklijke Marechaussee en het OM. De RvIG beschikt niet over opsporende of toezichthoudende bevoegdheden en moet dit overlaten aan de instanties.

Uit de Monitor Identiteit 2025 blijkt dat fraude met identiteitsgegevens zich voornamelijk afspeelt in het digitale domein. In meer of mindere mate speelt de RvIG volgens de huidige kaders een rol in de aanpak van het misbruik van ID-bewijzen. Het gaat om:

- Het vaststellen of verifiëren van de identiteit
- Het melden van identiteitsfraude
- Informatie-uitwisseling met partners
- Het gebruik van de app voor ID bewijzen en de invoering van de EDI-wallet (de Europese identiteit)

Binnen de RvIG richt het Centraal meldpunt identiteitsfraude zich op de ondersteuning van de individuele melder die vermoedens heeft over ID-fraude. In 2025 kwamen bijna negenduizend meldingen binnen.

Er worden door het CMI geen gegevens geregistreerd van de mogelijke dader, de melder wordt hiervoor doorverwezen naar de politie. Het CMI doet niet aan de zgn. warme doorverwijzing, dat betekent dat de melder zelf zich moet wenden bij andere meldpunten zoals de politie, de bank of een internetplatform tenzij dit nodig is voor de ondersteuning van de individuele melder.
Uit de workshops van het Programma over te plegen interventies bij online fraude is ID-fraude in de 'criminal journey' vastgesteld als het startpunt van diverse online fraudevormen. Er is nu geen sprake van een structurele informatie-uitwisseling met andere meldpunten en organisaties die ID-fraude signaleren zoals banken, verzekeraars, telecomproviders of de politie. De bij deze organisaties geregistreerde ID-fraude wordt niet gedeeld met het CMI. Het CMI heeft hiermee een deel van het overzicht van mogelijke ID-fraude.

In een toekomstig wetsvoorstel wordt het CMI het eerste wettelijk verankerde meldpunt op het gebied van online fraude. Hierin wordt de wettelijke taak van het CMI grotendeels gelijk aan de huidige situatie.

## 9. Financiële inlichtingen eenheid

De Financiële Inlichtingen Eenheid (FIU)[12] is op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme[13] (Wwft) het centrale meldpunt waar verschillende instellingen ongebruikelijke transacties rapporteren. De FIU werkt samen met publieke en private partners, zowel nationaal als internationaal, om witwassen, terrorismefinanciering en onderliggende delicten te voorkomen en te bestrijden. Doel is om de integriteit van het financiële stelsel te waarborgen. De FIU verzamelt financiële inlichtingen door nieuwe trends en fenomenen te signaleren en de partners hierover te informeren.

Op 6 december 2024 heeft de FIU de instructie verzonden met name gericht aan de banken, om de ongebruikelijke transacties te melden die betrekking hebben op 'betaalfraude of oplichting'. Dit met het doel 'een beter inzicht in en kansen voor de aanpak van zowel het witwassen van opbrengsten

12 Financial Intelligence Unit-Nederland (FIU-Nederland) https://www.fiu-nederland.nl/home/over-fiu/
13 https://wetten.overheid.nl/BWBR0024282/2026-01-01

uit (betaal)fraude en oplichting, als deze gronddelicten zelf'.[14] In deze instructie wordt gevraagd het fraudetype te melden en of de klant (en zo ja, welke klant) slachtoffer of begunstigde van de fraude/ oplichting is.

De FIU is daarmee een belangrijke 'verzamelplaats' van gegevens over online fraude die als ongebruikelijke transactie door de meldingsplichtigen zijn gedetecteerd. De FIU kan deze verkregen data analyseren en doorgeven aan de opsporingsautoriteiten. Online fraude oftewel oplichting wordt als een gronddelict gezien dat leidt tot witwassen.

In de toekomstige Europese verordening (AMLR) die in 2027 in werking treedt, komt een grondslag voor gegevensdeling in het kader van partnerschappen onder toezicht van de toezichthouder.

## 10. Kamer van Koophandel

De KVK heeft een aantal wettelijke taken die staan voor adviseren, beheren, voorlichten en stimuleren. Sinds april 2026 heeft de KVK een proactieve rol gekregen in de criminaliteitsbestrijding naar aanleiding van de AMLD6.
De KVK is daarmee niet langer alleen een beheerder van registers maar krijgt de rol van beoordelaar, controleur en toegangsverlener: de 'poortwachtersfunctie'. Belangrijke elementen van de poortwachtersrol van de KVK zijn:

- Weigeringsbevoegdheid
- Adrescontrole
- Identiteitsverificatie
- UBO-register: De KVK fungeert als poortwachter voor de registratie van Ultimate Beneficial Owners (UBO's)

De KVK onderzoekt hun rol op het terrein van online fraude in samenwerking met partners en het ontwikkelen van interventies.

14 https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2025/nieuwe-instructie-voor-het-melden-van-betaal-fraude-en-oplichting/

## 11. Gemeenten

De gemeenten zijn zich steeds meer gaan richten op de digitale veiligheid en weerbaarheid van hun inwoners en bedrijven. Zij volgen hiervoor de Agenda Digitale Veiligheid 2028 en het Regionale Veiligheidsplan. Een belangrijk instrument voor een gemeente is het cyber intel beeld om regionaal inzicht te krijgen in oa. digitale criminaliteit. Vanuit de VNG zijn meerdere instrumenten ontwikkeld om de gemeenten te helpen in gegevensdeling bijv. in het sociaal, zorg- en veiligheidsdomein.

Een bekend samenwerkingsverband is het Regionaal Informatie- en Expertisecentrum (RIEC) waarbinnen de deelnemers op grond van de WGS onder voorwaarden gegevens mogen delen.

## 12. Gegevensdeling en het slachtoffer

**Verstrekking door het slachtoffer**
Het slachtoffer speelt in de 'gegevensdeling' een belangrijke rol omdat hij een van de startpunten is van de informatieketen nl. door het doen van de aangifte of de melding. Uit de CBS-cijfers blijkt dat slechts 17% van de slachtoffers van online fraude aangifte doet bij de politie en 55% doet melding bij een andere instantie. In meerdere onderzoeken komt als aanbeveling naar voren om de kwaliteit en de registratie van de aangifte te verbeteren. Ook het centraliseren en analyseren van de informatievoorziening op basis van meldingen en aangiften die zich nu op verschillende plaatsen bevinden, zal volgens onderzoeksrapporten de datakwaliteit, detectie en opsporing ten goede komen.

Het slachtoffer kan bij meerdere meldpunten een melding doen, afhankelijk van type fraude of de hulpvraag. Bijv. bij de Fraudehelpdesk kan het slachtoffer de melding doen, geadviseerd en doorverwezen worden. Sinds kort loopt er een proef van samenwerking om de melder warm door te verwijzen naar de politie. Bij het Centraal meldpunt identiteitsfraude kan de melder zijn vermoeden van identiteitsfraude melden en ondersteuning krijgen. Ook bij de banken en webshops kunnen de cliënten hun vermoedens van online fraude melden.
Er is nu geen structurele gegevensdeling tussen meldpunten. Het uitwisselen van de gegevens tussen meldpunten verkregen uit de meldingen is afhankelijk van de beoordeling door de verstrekkende

organisatie. Bijv. of organisaties van de meldpunten willen meewerken, of de verstrekkende partij positief oordeelt over het gerechtvaardigd belang als algemene grondslag en of er sprake is van strafrechtelijke persoonsgegevens. In de meeste gevallen zal hiervoor geen uitzonderingsgrond zijn.

**Verstrekking aan het slachtoffer**

Het slachtoffer bevindt zich in een afhankelijkheidspositie om aan gegevens te komen. Er zijn meerdere routes en mogelijkheden maar die zijn vaak onbekend en niet makkelijk toepasbaar[15]. Gegevensdeling met het slachtoffer hangt af van oa. de organisatie waar het incident plaatsvond, de online fraudevorm, het meldpunt, de procedure. Hiervoor zijn geen wettelijke kaders.
Het lectoraat Cybercrime & Cybersecurity van De Haagse Hogeschool is in samenwerking met partners gestart met een onderzoeksproject waarin de civielrechtelijke afdoening van online fraude centraal staat. Een van de onderzoeken richt zich op de ervaringen van slachtoffers met deze vorm van schadeverhaal[16].
Een aantal PSP's hebben een module op hun website waar het slachtoffer gegevens kan opvragen over de begunstigde.[17]
De Procedure NAW-gegevens begunstigde Non-Bancaire Fraude biedt onder voorwaarden de mogelijkheid om de naam, adres, woonplaats (NAW) gegevens van de begunstigde te verkrijgen. Oa. geldt de eis dat er sprake is van drie aangiften op hetzelfde bankrekeningnummer en zowel de rekening van de betaler als van de begunstigde moet een Nederlands rekeningnummer zijn. Deze procedure is niet wettelijk geregeld. De banken hebben twijfels over de effectiviteit van deze procedure, hun rol hierin en de geheimhouding jegens hun klanten.

Een andere route voor het slachtoffer om aan gegevens te komen voor een civiel verhaal, is via een civiele rechtsvertegenwoordiger. De politie mag op grond van het Besluit politiegegevens[18], politiegegevens verstrekken aan een civiele vertegenwoordiger.

**Opvallende punten huidige kader**

## 13. Het vaststellen van het strafrechtelijk persoonsgegeven

Uit de casussen en de gehouden interviews blijkt dat het in de praktijk lastig is om het strafrechtelijk persoonsgegeven en de kring van personen op wie het gegeven betrekking heeft, vast te stellen. De omschrijving van artikel 10 AVG en artikel 1 UAVG geeft de praktijk weinig houvast om te bepalen of sprake is van een strafrechtelijk persoonsgegeven. De begrippen in de omschrijving leiden tot verschillende interpretaties. De jurisprudentie laat zien dat ook het doel, de context en de gevolgen voor de betrokkene bepalend zijn of de 'strafrechtelijke veroordeling' en 'het strafbare feit' onder artikel 10 AVG vallen. Volgens de criteria van de Hoge Raad is een persoonsgegeven niet snel een strafrechtelijk persoonsgegeven. Er moeten voldoende feiten zijn om een bewezenverklaring te onderbouwen. Volgens de 'guidelines' van de Engelse toezichthouder, de Information Commissioner's Office (ICO) gaat het bij strafrechtelijke persoonsgegevens alleen over daders en mogelijke daders (en niet het slachtoffer).[19]

15 Geld terugkrijgen na oplichting moet makkelijker
16 https://www.dehaagsehogeschool.nl/onderzoek/centres-expertise/civielrechtelijke-afdoening-van-online-fraude
17 Je geld terug na oplichting
Geld terugkrijgen na oplichting moet makkelijker

18 wetten.nl - Regeling - Besluit politiegegevens - BWBR0023086, art. 4:2 eerste lid onder n.
19 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-is-criminal-offence-data/ - victims

## 14. Het strafbare feit en het strafrechtelijk persoonsgegeven

Extra complicerend is dat het fenomeen online fraude in de praktijk allerlei vormen kent en niet direct overeenkomt met de delictsomschrijvingen in het Wetboek van Strafrecht. Online fraude als zodanig bestaat in het strafrecht niet als strafbaar feit. Uit onderzoek blijkt dat de rechtspraak gebruik maakt van 20 delictsomschrijvingen om tot een veroordeling te komen. 'Oplichting' kent een zware bewijslast en voor 'online handelsoplichting' is een structureel gedrag nodig: 1 keer online handelsoplichting is niet genoeg om tot een veroordeling te komen.
De Hoge Raad heeft een nadere omschrijving gegeven van het strafrechtelijk persoonsgegeven zoals hierboven vermeld. Dit betekent dat organisaties in de praktijk de relatie moeten leggen tussen de fraudevormen uit de praktijk en het juridisch strafbare feit. Criteria als 'aangiftewaardig' of 'voldoende bewijs' verwijzen naar wettelijke delictsomschrijvingen die niet altijd overeenkomen met de criteria die organisaties in de praktijk bij online fraude hanteren. Beide hebben een ander doel maar komen samen als het strafrechtelijk persoonsgegeven bepaald moet worden. Dit bemoeilijkt het vaststellen van het strafrechtelijk persoonsgegeven waar de verwerkingsverantwoordelijke over 'met feiten onderbouwd bewijs' moet beschikken gericht op de formele delictsomschrijvingen.

## 15. De vergunningverlening door de AP

De meeste vergunningen van de AP zijn gericht op fysieke criminaliteit en een geografisch begrensd gebied nl. een winkel- en uitgaansverbod. Van de 500 verleende vergunningen voor de deling van strafrechtelijke persoonsgegevens heeft de AP tot nu toe drie vergunningen verleend voor een geautomatiseerde database of register met verwijzingen naar 'veiligheidsincidenten'. Het gaat om het Protocol incident waarschuwingssysteem financiële instellingen (PIFI)[20], Ugly Mugs (een waarschuwingsregister voor sekswerkers) en het Protocol Gatekeeper voor de beveiliging van de havens.

De randvoorwaarden in deze vergunningen zijn oa. dat de gegevensdeling sectoraal is, via een tussenschakel zoals een stichting of een veiligheidsafdeling, op hit-no hit basis en op incidentniveau. Het geografisch gebied betreft Nederland. Met deze sectorale vergunningen kunnen geen databestanden van bijv. gelekte accounts of valse bankrekeningnummers tussen private organisaties worden vergeleken.

## 16. Het vergunningenstelsel en cross sectorale gegevensdeling

In de Handreiking Cross-sectorale gegevensdeling private partijen stelt de AP zich op het standpunt dat cross sectoraal delen tussen private partijen van gegevens op een zwarte lijst niet is toegestaan. De AP stelt dat '*de kans zeer klein is dat de AP een vergunning verleent om strafrechtelijke gegevens (zoals over fraude of diefstal) cross-sectoraal te delen met volstrekt andere branches of sectoren*'[21]. De AP beroept zich op de wetsgeschiedenis van de vergunningverlening waaruit volgt dat het vergunningstelsel bedoeld is voor gegevensuitwisseling binnen een bepaalde branche of in een afgebakend geografisch gebied. De indruk die hier ontstaat, is dat het vergunningenstelsel niet aansluit op de digitale platforms met meerdere partijen en een integrale aanpak. De AP heeft de voorkeur voor wetgeving en een democratisch proces op basis waarvan gegevensdelingen met een grote impact, worden gelegitimeerd. In het evaluatierapport van de UAVG[22] wordt de vraag opgeworpen of cross sectorale gegevensdeling tussen private partijen door middel van vergunningverlening door de toezichthouder geregeld kan worden. Dit gelet op de grote impact op betrokkenen en de waarborgen die vereist zijn. In het evaluatierapport wordt de suggestie voor wetgeving met de nodige waarborgen gedaan.[23]

20 Banken - hypotheekverstrekkers - financieringsondernemingen en (zorg)verzekeraars aangesloten bij branchaeverenigingen.

21 Handreiking Cross-sectorale gegevensdeling private partijen, Autoriteit Persoonsgegevens, 15 juli 2021, Handreiking cross-sectorale zwarte lijsten | Autoriteit Persoonsgegevens, artikel 33, vierde lid, aanhef en onder c UAVG

22 Rapport, Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid, Pro Facto en Hooghiemstra en Partners in opdracht van het WODC, juni 2022 https://www.wodc.nl/actueel/nieuws/2022/09/06/uitvoeringswet-avg-kritisch-beoordeeld

23 Brief Tweede Kamer, Verwerking en bescherming persoonsgegevens, kamerstuk 32 761, nr. 284, 18 september 2023 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2023Z15374&did=2023D37335

## 17. Waarborgen betrokkene over wie gegevens gedeeld worden

Een wettelijk vereiste[24] voor het verwerken van persoonsgegevens of bij het verwerken van strafrechtelijke persoonsgegevens is het treffen van passende waarborgen. De betrokkene over wie gegevens gedeeld worden, loopt het risico uitgesloten en/of gestigmatiseerd te worden en kan door meerdere maatregelen tegelijkertijd getroffen worden. Dit is naast de rechten van een betrokkene die in de AVG, de UAVG en de Wpg zijn geregeld zoals het recht op inzage of verwijdering.

In de praktijk bestaan diverse voorbeelden van waarborgen voor de positie van de betrokkene over wie gegevens gedeeld worden. In de WGS, de vergunningverlening van de AP en in het PIFI zijn meerdere waarborgen te vinden bijv.: het beperken van de kring van deelnemers, een procedure om uit een register te komen, een coördinerend functionaris gegevensbescherming, een veiligheidsafdeling die de verstrekking beoordeelt en een reguliere audit op de verwerking.

Er zijn meerdere projecten waar Privacy Enhanced Technology[25] (PET) als waarborg wordt toegepast. Toelichting:

In de Wet bevorderen samenwerking en rechtmatige zorg[26] worden het Waarschuwingsregister zorgfraude en het Informatieknooppunt Zorgfraude (IKZ) geregeld. In nadere regelgeving worden oa. de gerechtvaardigde overtuiging van fraude en het informeren van de betrokkene uitgewerkt.

Voor gegevensdeling online fraude zijn waarborgen nodig die passend zijn bij de specifieke kenmerken van online fraude.  Het gaat oa. de verschillende typen organisaties, de impact van hun maatregelen op een betrokkene en de internationale gevolgen. Waarborgen die in een protocol opgenomen zouden kunnen worden zijn oa. de criteria van ‘gerechtvaardigde overtuiging’, criteria van deling, de toepassing van Multi Partition Computation (MPC), het informeren van de betrokkene, het bezwaar door de betrokkene die in het register is opgenomen, monitoring samenloop van maatregelen, de voorwaarden van gegevensdeling met de politie en de vormen van internationale samenwerking.

### Overzicht

**Wat is mogelijk in het huidige kader om gegevens over online fraude te delen?**

1. Modus operandi kunnen binnen en tussen sectoren en publieke organisaties gedeeld worden zolang deze niet direct of indirect herleidbaar zijn tot een individu.
2. In de mini-keten verwerkingen (bijv. een webshop, vervoerder en betaaldienstverlener) is een gegevensdeling van een minimale set aan gewone gegevens mogelijk om een vermoedelijke frauduleuze transactie te blokkeren. Hier moet wel aan een aantal eisen zijn voldaan. Dit kan op grond van een overeenkomst of op grond van het gerechtvaardigd belang. Daarvoor is een belangrijk vereiste dat de positie van de betrokkene voldoende is geborgd. Deze vorm van gegevensdeling kan in de praktijk verschillend beoordeeld worden. Dit kan voorkomen worden door een uitvoeringsprotocol.
3. Deling van strafrechtelijke persoonsgegevens met derden is mogelijk met een vergunning van de AP als de andere uitzonderingsgronden in de UAVG niet aan de orde zijn zoals een sectorale wet. De banken en verzekeraars beschikken reeds over een vergunning van de AP voor het delen strafrechtelijke persoonsgegevens via een extern verwijsregister, volgens het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI).[27]

24 Bijv. bij een verdere verwerking op grond van artikel 6, vierde lid, sub e, AVG of artikel 10, 24 en 25 AVG.

25 Privacy Enhanced Technology is een overkoepelende term voor verschillende technieken die betere gegevensbescherming mogelijk maken. PET maakt het mogelijk om analyses op data te doen zonder dat (persoons) gegevens in leesbare vorm worden uitgewisseld.

26 https://zoek.officielebekendmakingen.nl/stb-2023-285.html, Wet van 25 augustus 2023, Stb. 2023, 285

27 Per 1 april 2026 is een nieuwe versie van het PIFI in werking getreden. https://www.nvb.nl/publicaties/protocollen-regelingen-richtlijnen/protocol-incidenten-waarschuwingssysteem-financiele-instellingen-pifi/

4. In een samenwerkingsverband met de politie zoals de Electronic Crimes Task Force (ECTF) en het Landelijk meldpunt internetoplichting (LMIO) delen private organisaties persoonsgegevens met de politie en het OM via een aangifte of een vordering. Dit ervaart men als een beperking in het detecteren van netwerken en relaties in de onderzoeksfase. Overweging 50 van de AVG verwijst naar het gerechtvaardigd belang om persoonsgegevens met de lokale autoriteiten te delen. Dit wordt op verschillende manieren geïnterpreteerd. Als aan de eisen van het gerechtvaardigd belang is voldaan, zou deze grondslag voldoende kunnen zijn voor gewone en strafrechtelijke persoonsgegevens. Guidance van de AP is nodig om hier duidelijkheid in te krijgen.
5. In een samenwerkingsverband dat valt onder de WGS, zoals de taskforces onder het FEC, is het onder zeer strikte restricties mogelijk om tussen de publieke en private partijen informatie te delen.
6. De telecommunicatie aanbieder kan op grond van de Telecommunicatiewet met de politie en OM verkeersgegevens delen met het oog op de voorkoming, opsporing en vervolging van strafbare feiten.
7. De politie verstrekt gegevens aan een civiele rechtsvertegenwoordiger van een slachtoffer, op grond van art. 18 lid 1 Wpg in combinatie met art. 4:2 lid 1 Besluit politiegegevens.
8. De debet bank verstrekt aan het slachtoffer onder voorwaarden de gegevens van de begunstigde om een civiele procedure te starten volgens de Procedure NAW-gegevens Begunstigde bij niet-bancaire Fraude (PNBF). Oa. moeten er meer dan drie aangiften zijn gedaan, de credit PSP moet een andere zijn dan de debet PSP, het gaat alleen om Nederlandse bankrekeningen en de begunstigde heeft na 24 dagen het geld nog niet terugbetaald, dan worden de NAW-gegevens van de begunstigde verstrekt.
9. Een Collecting Payment Service Provider (CPSP) met een Nederlandse vergunning verstrekt gegevens over de begunstigde aan een slachtoffer, veelal via een module op de eigen website.

**Wat is niet mogelijk of onzeker in het huidige kader om gegevens over online fraude te delen?**

1. Het cross sectoraal delen van lijsten met strafrechtelijke persoonsgegevens bijv. over verdachte afleveradressen, bankrekeningnummers of apparaten, is niet mogelijk in het huidige kader. Hiervoor is geen sectorale wet noch een vergunning van de AP. Vergunningverlening door de AP voor cross sectoraal delen van strafrechtelijke persoonsgegevens is door de AP vrijwel uitgesloten.
2. Voor de webshops, betaaldienstverleners en vervoerders is geen vergunning van de AP of sectorale wet die gegevensdeling mogelijk maakt.
3. Meldingen over online fraude die bij verschillende private en publieke organisaties door meldpunten worden geregistreerd, met strafrechtelijke persoonsgegevens, mogen niet gedeeld worden. Hiervoor is geen sectorale wet die een uitzonderingsgrond creëert.
4. In de bestaande samenwerkingsverbanden tussen politie en private partners verstrekken de private partners volgens het afgesproken convenant geen strafrechtelijke of gewone persoonsgegevens aan de politie zonder aangifte. Ook private partners delen onderling in het samenwerkingsverband volgens het convenant geen persoonsgegevens over fraude incidenten.
5. Telecommunicatie aanbieders delen nu geen verkeersgegevens met elkaar of met andere private partners om online fraude tegen te gaan. De Telecommunicatiewet biedt hiervoor geen ruimte. Het delen van verkeersgegevens over verdachte apparaten met telecommunicatie aanbieders en met andere private partners is nu niet mogelijk.

Dit is een uitgave van:
**Ministerie van Justitie en Veiligheid**
Integrale aanpak online fraude

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH  Den Haag

**Voor meer informatie:**
integraleaanpakonlinefraude@minjenv.nl
integraleaanpakonlinefraude.nl

Juni 2026

Integrale aanpak
**online fraude**