PARLEMENT & WETENSCHAP

Opsporing en vervolging van onlinefraude onder het huidige en nieuwe wetboek van strafvordering

16 mei 2025 | mr. dr. Sanne Buisman, dr. Maša Galič, LL.M. (beiden Vrije Universiteit Amsterdam)[1]

NB: de hyperlinks in de samenvatting verwijzen naar de betreffende onderdelen in de factsheet.

Samenvatting

De digitalisering van de samenleving heeft geleid tot een *sterke toename van onlinefraude*. Zo berichtte CBS dat in 2024 1,4 miljoen personen slachtoffer zijn geworden van één of meer vormen van onlinefraude. Onlinefraude heeft een grote financiële, emotionele en psychische impact op slachtoffers en leidt tot verlies aan vertrouwen in het economische systeem en het maatschappelijke verkeer. Ondanks dat er steeds meer gevallen van onlinefraude zijn, is de aangiftebereidheid onder slachtoffers laag (§ 1).

Onlinefraude is een *containerbegrip* voor bedrog gericht op financieel gewin, die zonder ICT niet mogelijk zou zijn geweest (§ 2.1). In het fenomeenbeeld van onlinefraude kunnen *verschillende vormen van onlinefraude* worden onderscheiden, zoals aan- en verkoopfraude, bankhelpdeskfraude, hulpvraagfraude, betaalverzoekfraude, bankphishing en beleggingsfraude (§ 2.2).

Onder het Wetboek van Strafrecht zijn er diverse strafbepalingen die gebruikt worden om vormen van onlinefraude te *vervolgen*. Daarbij kan worden gedacht aan computervredebreuk, oplichting, witwassen en valsheid in geschrifte. Deze delicten maken het mogelijk om ook meer *ingrijpende opsporingsbevoegdheden in te zetten* om de verdachten van deze strafbare feiten op te sporen (§ 2.3).

Het huidige Wetboek van Strafvordering bevat een groot aantal opsporingsbevoegdheden waarvan gebruik kan worden gemaakt voor de opsporing van onlinefraude. Nu onlinefraude zich voornamelijk in de digitale omgeving afspeelt, vallen veel van deze opsporingsbevoegdheden onder de zogenoemde digitale opsporing. De belangrijkste bevoegdheden zijn het *vorderen van identificerende en verkeersgegevens*, *doorzoeking van geautomatiseerde werken*, *netwerkzoeking tijdens het doorzoeken van plaatsen*, *aftappen van communicatie* en de *hackbevoegdheid*. Daarnaast zijn de bevoegdheden inzake het *ontoegankelijk maken van gegevens* van belang bij de bestrijding van onlinefraude (§ 3).

Onder het *nieuwe Wetboek van Strafvordering* wordt de regeling voor de digitale opsporing volledig geherstructureerd, waarbij het onderzoek van gegevens een centrale positie krijgt. 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. 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 de *netwerkzoeking na inbeslagname*, waarmee reeds ervaring is opgedaan onder de Innovatiewet Strafvordering en waarvan de evaluaties positief zijn.

[1] Deze bijdrage is tot stand gekomen met medewerking van Jan Winnubst, student-assistent bij de Afdeling Strafrecht van de Vrije Universiteit, die in dat kader de verschillende schematische overzichten in de bijlagen heeft geconcipieerd.

Tevens kunnen het bevel *data-analyse door een derde* en de *stelselmatige locatiebepaling* van belang zijn in de opsporing van onlinefraude (§ 4).

Hoewel het straf(proces)recht dus verschillende mogelijkheden bevat in onlinefraude op te sporen en te vervolgen, is de aanpak van onlinefraude niet louter een strafrechtelijke aangelegenheid. Juist een *integrale aanpak van onlinefraude*, waarbij verschillende rechtsgebieden, actoren en middelen en maatregelen worden ingezet, kan uitkomst bieden. Daarbij is een belangrijk aandachtspunt dat het recht op *gegevensbescherming* van personen voldoende wordt gewaarborgd (§ 5).

1. Inleiding

Door de digitalisering van de samenleving is in de afgelopen jaren het aantal gevallen van onlinefraude sterk toegenomen. Burgers, bedrijven en overheden zijn in grote mate afhankelijk van digitale systemen voor communicatie, financiële transacties, handel en opslag van gevoelige informatie. Dit biedt voor criminelen nieuwe kansen voor vormen van online criminaliteit.[2] In 2024 werden 2,4 miljoen personen slachtoffer van één of meer vormen van onlinefraude.[3] De financiële schade omvatte in 2023 ruim 100 miljoen euro.[4] De omvang van de verschillende vormen van onlinefraude verschilt naar type. Veruit de meeste registraties hadden betrekking op aan- en verkoopfraude (42.359), bankhelpdeskfraude (6.970).[5] Onlinefraude heeft een grote financiële, emotionele en psychische impact op slachtoffers en leidt tot verlies aan vertrouwen door burgers, bedrijven en overheden in het economische systeem en het maatschappelijke verkeer.[6] Ondanks dat er steeds meer gevallen van onlinefraude zijn, is de aangiftebereidheid onder slachtoffers beperkt.[7] Schaamte speelt een grote rol in de terughoudendheid van slachtoffers om melding te maken.[8]

Sinds 2022 wordt door de overheid ingezet op een integrale aanpak van onlinefraude, waarbij wordt aangestuurd op hybride handhaving door middel van de inzet van verschillende rechtsgebieden, zoals het privaatrecht, bestuursrecht en het strafrecht.[9] In deze factsheet ligt de focus op de strafrechtelijke handhaving van onlinefraude. In dat kader staan de volgende twee vragen centraal:

1. Welke bevoegdheden hebben de autoriteiten om onlinefraude op te sporen en te vervolgen onder het huidige Wetboek van Strafvordering?
2. Wat verandert er onder het nieuwe Wetboek van Strafvordering in de opsporing en vervolging van onlinefraude en in hoeverre zullen deze wijzigingen bijdragen aan de effectiviteit van de aanpak van onlinefraude?

Om deze vragen te beantwoorden zal allereerst 'onlinefraude' worden geconceptualiseerd. Daartoe wordt eerst een definitie gegeven van onlinefraude. Vervolgens wordt inzichtelijk gemaakt op basis van welke artikelen van het Wetboek van Strafrecht kan worden vervolgd (§ 2). In § 3 wordt vervolgens in kaart worden gebracht op welke wijze onlinefraude kan worden opgespoord. Bij de opsporing (en in bredere zin bestrijding) van onlinefraude spelen vooral digitale opsporingsbevoegdheden die elektronisch bewijs opleveren een belangrijke rol. In deze paragraaf worden daarom de volgende digitale bevoegdheden besproken: het vorderen van gegevens (§ 3.1), de doorzoeking van geautomatiseerde werken (§ 3.2), de netwerkzoeking tijdens (§ 3.3), het aftappen van communicatie (§ 3.4) en de hackbevoegdheid (§ 3.5). Tevens wordt ingegaan op de bevoegdheid tot het ontoegankelijk maken van gegevens (§ 3.6). Daarna zal een overzicht worden gegeven van de veranderingen die worden doorgevoerd onder het nieuwe Wetboek van Strafvordering (§ 4). In deze paragraaf wordt allereerst het nieuwe algemene kader voor digitale opsporing geschetst (§ 4.1). Vervolgens wordt nader ingegaan op de bevoegdheid kennisnemen gegevens na inbeslagname (§ 4.2.1) en de netwerkzoeking na inbeslagname (§ 4.2.2), waarmee reeds ervaring is opgedaan onder de Innovatiewet Strafvordering. Daarna worden de nieuw in te voeren

---

[2] *Online fraude in beeld. Fenomeenbeeld 2024*, Politie 2024, via www.politie.nl, p. 3.

[3] CBS, 'Online oplichting en fraude', *Online Veiligheid en Criminaliteit 2024*, 15 april 2025, via www.cbs.nl.

[4] Politie 2024 (vnt. 2), p. 3. Voortgangsrapportage Integrale Aanpak Online Fraude, 28 juni 2024, p. 1.

[5] Politie 2024 (vnt. 2), p. 3. Voortgangsrapportage Integrale Aanpak Online Fraude, 28 juni 2024, p. 1.

[6] Politie 2024 (vnt. 2), p. 3. Zie ook CBS 2024 (vnt. 3). S.S. Buisman, 'Kwalitatieve en transparante fraudebestrijding. Een verkennend onderzoek naar handhavingscriteria voor fraudedelicten', *TBS&H* 2021, nr. 6, p. 359. Vgl. B. Bloem & A. Harteveld, *Horizontale fraude. Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012*, Zoetermeer: Politie 2012.

[7] Zie M. Akkermans, E. Derksen, M. Kennis, R. Kloosterman & E. Moons, *Veiligheidsmonitor 2023*, Centraal bureau voor de statistiek, via www.cbs.nl, par. 5.4. In 2023 werd 46% van de gevallen gemeld bij een instantie, slechts 17% heeft daadwerkelijk aangifte gedaan. In 2024 werd 47% van de gevallen gemeld bij een instantie. Slechts 21% deed aangifte. Zie CBS 2024 (vnt. 3).

[8] Zie Bloem & Harteveld 2012 (vnt. 6).

[9] *Kamerstukken II,* 2022/21, 29911, nr. 341. Buisman 2021 (vnt. 6), p. 6.

bevoegdheden van het bevel tot data-analyse door een derde (§ 4.3.1) en stelselmatige locatiebepaling (§ 4.3.2) besproken. De factsheet sluit af met een conclusie en enkele reflecties (§ 5).

2. Wat is onlinefraude?

2.1. Definitie van onlinefraude

Fraude is een zeer breed en moeilijk te definiëren begrip. Het betreft een verzamelbegrip waar heel veel verschillende vormen van oneerlijk en bedrieglijk gedrag onder vallen. Hoewel het begrip 'fraude' vaak een strafrechtelijke connotatie heeft, hoeft fraude niet altijd tot strafrechtelijke consequenties te leiden.[10] Binnen de strafrechtelijke context wordt fraude veelal omschreven als opzettelijke misleiding om onrechtmatig voordeel te verkrijgen.[11] Binnen het Wetboek van Strafrecht is echter geen overkoepelende definitie van fraude gegeven. Fraude fungeert hier dus als containerbegrip waaronder verschillende soorten delicten kunnen worden gebracht.[12]

Fraude kan worden onderscheiden in verticale en horizontale fraude. Bij verticale fraude is sprake van gevallen waarbij de overheid wordt benadeeld, zoals in geval van belasting- en sociale zekerheidsfraude en subsidiefraude.[13] In geval van horizontale fraude, richten fraudeurs zich op burgers, bedrijven en organisaties. Daarbij kan gedacht worden aan beleggingsfraude, hypotheekfraude, verzekeringsfraude etc.[14]

Onlinefraude, ook wel aangeduid als 'online oplichting', 'internetfraude' of 'internetoplichting',[15] wordt daarom ook wel gedefinieerd als 'bedrog met als oogmerk het behalen van financieel gewin, waarbij ICT essentieel is voor de uitvoering'.[16] Het gaat dus steeds om frauduleuze feiten die niet gepleegd zouden kunnen zijn op dezelfde of een zeer vergelijkbare wijze zonder gebruik van online technologie. De verdere digitalisering van de samenleving heeft ertoe geleid dat ook de vormen van horizontale fraude zijn gedigitaliseerd. Voor veel oplichters bieden e-mail, telefoon en communicatieapps een eenvoudige manier om grootschalig potentiële slachtoffers te bereiken.[17] Bovendien zijn door de opkomst van sociale media veel persoonlijke gegevens openbaar en kan eveneens inzicht worden verkregen in het sociale netwerk van personen, welke informatie door fraudeurs kan worden gebruikt bij hun oplichtingspraktijken.[18]

2.2. Aard en omvang van onlinefraude in Nederland

In het fenomeenbeeld van de politie inzake onlinefraude worden de verschillende verschijningsvormen van onlinefraude in Nederland in kaart gebracht. In 2023 werden de volgende vormen en aantallen van onlinefraude geregistreerd[19]:

1. *Aan- en verkoopfraude (42.359 gevallen);*
   Deze vorm van fraude staat ook wel bekend als marktplaatsoplichting of flessentrekkerij. Oplichters bieden producten aan en vragen daarbij om een vooruitbetaling, maar leveren vervolgens niet (aankoopfraude/marktplaatsoplichting). Zij kunnen ook producten bestellen of kopen en vragen daarbij om vooruitlevering, maar betalen volgens niet (koopfraude/marktplaatsoplichting).[20]

[10] S.S. Buisman, *Contract, tort & crime* (diss. Tilburg), Studio: Tilburg 2019, p. 11. Zo kan fraude bij tentamens of scripties bij de universiteit bijvoorbeeld leiden tot ongeldigverklaring van het resultaat of in zeer ernstige gevallen tot uitsluiting van de opleiding.

[11] Deze omschrijving is ontleend aan het openbaar ministerie, zie www.om.nl (laatst geraadpleegd 30 april 2025). Vgl. Buisman 2021 (vnt. 6), p. 359.

[12] C.A. Meerts, S.S. Buisman, W. Huisman, M. de Groodt & S.A.T. de Jong, *Zelfonderzoek en zelfmelden van fraude en corruptie door bedrijven*, Den Haag: WODC 2023, p. 3.

[13] Politie 2024 (vnt. 2), p. 22.

[14] Politie 2024 (vnt. 2), p. 22. Zie bijvoorbeeld Bloem & Harteveld 2012 (vnt. 6).

[15] E.R. Leukfeldt, M.M.L. Domenie, W.Ph. Stol, W. Ph. (2010) *Verkenning cybercrime in Nederland* 2009, Den Haag: Boom Juridische Uitgevers 2010. E.R. Leukfeldt & W.Ph. Stol, *Internetoplichters uitgelicht. E-fraudeurs en klassieke fraudeurs vergeleken*, De Bilt/Leeuwarden: Programma Aanpak Cybercrime / NHL Hogeschool 2011.

[16] J. Jansen, S. Westers, S. Twickler, W. Stol, Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing, Politie & Wetenschap 2019.

[17] Politie 2024 (vnt. 2), p. 22.

[18] Politie 2024 (vnt. 2), p. 22.

[19] Informatie ontleend aan Politie 2024 (vnt. 2). In dit fenomeenbeeld is ook het fenomeen sextortion opgenomen. Sextortion is echter een vorm van online bedreiging, intimidatie en/of afpersing en past daarom minder goed binnen de categorie van online fraude. Daarom is dit fenomeen in deze factsheet verder buiten beschouwing gelaten. Voor meer informatie over sextortion zie p. 100 e.v. Zie ook CBS, *Veiligheidsmonitor 2023 – Online criminaliteit*, via www.cbs.nl: in 2023 ging het aantal gevallen van online fraude omlaag van 9,7% naar 9,3%.

[20] Politie 2024 (vnt. 2), p. 34. Zie ook CBS 2023 (vnt.19): in 2023 bleef het aantal gevallen van online aankoopfraude (6,9%) en verkoopfraude (1,4%) gelijk. Zie uitgebreid over deze vorm van fraude S.S. Buisman, *Contract, tort & crime* (diss. Tilburg), Studio: Tilburg 2019.

2. *Bankhelpdeskfraude (6.970 gevallen);*
   In het geval van bankhelpdeskfraude wordt het slachtoffer opgebeld door personen die zich voordoen als een medewerker van de bank. Slachtoffers wordt verteld dat hun geld veilig moet worden gesteld door het geld naar een andere rekening over te maken, die in werkelijkheid onder controle van de oplichters staat.[21]
3. *Hulpvraagfraude (5.981 gevallen);*
   Bij hulpvraagfraude ontvangen slachtoffers uit naam van een bekende de vraag of zij snel een betaling kunnen doen. Het geld wordt vervolgens overgemaakt aan de oplichter of een katvanger.
4. *Betaalverzoekfraude (4.000);*
   Betaalverzoekfraude is een vorm van phishing, waarbij de oplichting eerst een betaalverzoek stuurt van 1, 2 of 5 cent onder het voorwendsel dat zij eerder zijn opgelicht en zeker willen weten dat het goed zit. De link van het betaalverzoek is vervolgens gekoppeld aan een malafide website. Op deze site wordt vervolgens om allerlei persoonsgegevens gevraagd, waarmee de oplichters toegang kunnen verkrijgen tot de bankrekening van het slachtoffer.[22]
5. *Misbruik accounts voor bestellingen (3.094);*
   Bij deze vorm van onlinefraude maakt de oplichter misbruik van de persoonsgegevens van het slachtoffer om zo een webshopaccount aan te maken. Vervolgens worden op dit account producten en/of diensten afgenomen uit naam van de klant en de daaraan gekoppelde creditcard, tegoedkaart of mogelijkheid om achteraf te betalen. De pakketjes worden vervolgens opgehaald bij een afhaalpunt, afgevangen door katvangers of afgeleverd door een bij de oplichtingspraktijk betrokken chauffeur van een bezorgdienst.[23]
6. *Bankphishing (2.700 gevallen);*
   Bij bankphishing wordt aan slachtoffers een link verstuurd die afkomstig lijkt te zijn van een bank. Door te klikken op de link wordt het slachtoffer doorgeleid naar een malafide website, waar wordt gevraag om persoonlijke inloggegevens. Met deze gegevens wordt toegang verkregen tot de bankrekening van het slachtoffer.[24]
7. *Beleggingsfraude (1.500);*
   Beleggingsfraude kan zich op verschillende manieren voordoen. De meest bekende varianten zijn boillerroomfraude, ponzi-zwendel en piramidespelen. Potentiële slachtoffers worden overgehaald om hun geld te beleggen waarbij hoge rendementen in het vooruitzicht worden gesteld, in de meeste gevallen zien de slachtoffers niets terug van hun investeringen.[25]
8. *Tech support scam (545);*
   Bij tech support scams doet de oplichter zich voor als een medewerker van een belend softwarebedrijf. Er wordt het slachtoffer verteld dat er technische problemen zijn met zijn computer, e-mail of sociale media-accounts. Het slachtoffer dient vervolgens een Remote access Tool te installeren, zodat het probleem op afstand kan worden opgelost. Met de tool wordt vervolgens toegang verkregen tot de computer en daarmee ook tot de bankrekening van het slachtoffer.[26]
9. *CEO-fraude (326);*
   Bij CEO-fraude doet de oplichter zich voor als een hooggeplaatste bestuursfunctionaris. Uit naam van deze functionaris worden vervolgens betaalopdrachten verstuurt naar de financiële afdeling binnen de organisatie.[27]
10. *Factuurfraude (228).*
    Bij digitale factuurfraude verschaft de oplichter zich toegang tot een bestaande digitale factuur van een bedrijf, past het bankrekeningnummer aan en stuurt de factuur nogmaals naar de ontvanger vanuit een nagenoeg lijkend e-mailadres (vaak één letter verschil).[28]

2.3. Vervolging van onlinefraude

De hiervoor genoemde vormen van fraude kunnen onder verschillende bepalingen van het Wetboek van Strafrecht worden vervolgd. Om in kaart te brengen voor welke strafbare feiten wordt vervolgd in geval van onlinefraude is voor deze factsheet een verkennend rechtspraakonderzoek verricht.

[21] Politie 2024 (vnt. 2), p. 66. Zie ook CBS 2023 (vnt.19) en CBS 2024 (vnt. 3).
[22] Politie 2024 (vnt. 2), p. 46. Zie ook CBS 2023 (vnt.19) en CBS 2024 (vnt. 3).
[23] Politie 2024 (vnt. 2), p. 130. Zie ook CBS 2023 (vnt.19) en CBS 2024 (vnt. 3).
[24] Politie 2024 (vnt. 2), p. 42. Zie ook CBS 2023 (vnt.19). CBS 2024 (vnt. 3).
[25] Politie 2024 (vnt. 2), p. 114. Zie ook CBS 2023 (vnt.19). CBS 2024 (vnt. 3).
[26] Politie 2024 (vnt. 2), p. 22. Zie ook CBS 2023 (vnt.19). CBS 2024 (vnt. 3).
[27] Politie 2024 (vnt. 2), p. 22. Zie ook CBS 2023 (vnt.19). CBS 2024 (vnt. 3).
[28] Politie 2024 (vnt. 2), p. 22. Zie ook CBS 2023 (vnt.19). CBS 2024 (vnt. 3).

Daarbij is gezocht binnen strafrecht op onlinefraude op rechtspraak.nl. In totaal werden 395 uitspraken gevonden, waarbij er via systematische analyse van 142 uitspraken het oordeel van de rechter is bestudeerd. Het gaat in deze analyse steeds om frauduleuze handelingen die niet gepleegd zouden zijn op dezelfde of (zeer) vergelijkbare wijze zonder gebruik van online technologie. Uit deze rechtspraakanalyse komt naar voren dat in de meeste gevallen wordt vervolgd voor:

- *Computervredebreuk (artikel 138ab Sr);*

  Dit betreft het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan. Hiervan is in ieder geval sprake als de toegang tot het werk wordt verworven door het breken van beveiliging, door een technische ingreep, met behulp van valse sleutels of signalen of door het aannemen van een valse hoedanigheid. Een strafverzwaringsgrond kan zijn dat de dader vervolgens gegevens overneemt, aftapt of opneemt.

- *Wederrechtelijk plaatsen opname-, aftap- c.q. afluisterapparatuur (artikel 139d Sr);*

  Het beschikken over een technisch hulpmiddel dat hoofdzakelijk geschikt is tot het plegen van een misdrijf als computervredebreuk (artikel 138ab, eerste lid Sr), spam of bombing (artikel 138b Sr) of aftappen van gegevens die worden overgedragen via telecommunicatie (artikel 139c Sr), met het oogmerk om een zodanig misdrijf te plegen, of het beschikken over toegangscodes of vergelijkbare gegevens met het oogmerk om een zodanig misdrijf te plegen.

- *Verwerven of openbaar maken niet-openbare gegevens (artikel 139g Sr);*

  Het verwerven of voorhanden hebben van niet-openbare gegevens terwijl het redelijkerwijs moet worden vermoed dat deze gegevens zijn verkregen door een misdrijf, of het ter beschikking stellen, bekend maken, of uit winstbejag voorhanden hebben van niet-openbare gegevens terwijl redelijkerwijs vermoed moet worden dat zij uit een misdrijf verkregen zijn.

- *Deelname aan een criminele organisatie (artikel 140 Sr);*

  Het deelnemen aan een organisatie die tot oogmerk heeft het plegen van misdrijven. Ook het voortzetten van een organisatie na onherroepelijke verbodenverklaring van die organisatie door de rechter valt hieronder.

- *Valsheid in geschrifte (artikel 225 en 226 Sr);*

  Het valselijk opmaken of vervalsen van een geschrift bestemd om tot bewijs van enig feit te dienen met het oogmerk om het als echt en onvervalst te gebruiken of door anderen te doen gebruiken. Ook het opzettelijk gebruikmaken van het valse of vervalste geschrift als ware het echt en onvervalst, alsmede het opzettelijk afleveren of voorhanden hebben van een dergelijk geschrift, terwijl redelijkerwijs moet worden vermoed dat het bestemd is voor zodanig gebruik, valt hieronder.

- *Nalaten tijdig gegevens te verstrekken (artikel 227b Sr);*

  Het in strijd met een wettelijk voorschrift opzettelijk nalaten tijdig benodigde gegevens te verstrekken, waarbij het feit kan strekken tot bevoordeling van zichzelf of een ander, terwijl redelijkerwijs moet worden vermoed dat de gegevens van belang zijn voor de vaststelling van recht op een verstrekking of tegemoetkoming, of de hoogte of duur daarvan. Ook valt hieronder het in strijd met een wettelijk voorschrift opzettelijk nalaten van het tijdig verstrekken van benodigde gegevens, waarbij het feit kan strekken tot bevoordeling van zichzelf of een ander, terwijl redelijkerwijs moet worden vermoed dat de gegevens van belang zijn voor de vaststelling van af te dragen middelen aan een overheidsinstantie.

- *Misbruik identificerende persoonsgegevens (artikel 231b Sr);*

  Het opzettelijk en wederrechtelijk gebruiken van identificerende persoonsgegevens, niet zijnde biometrische persoonsgegevens, met het oogmerk om de eigen identiteit of die van een ander te verhelen of te misbruiken, waardoor uit dat gebruik enig nadeel kan ontstaan.

- *Stoffen of voorwerpen tot vervalsen bestemd (artikel 234 Sr);*

  Het beschikken over voorwerpen of gegevens waarvan de dader weet dat zij bestemd zijn tot het plegen van valsheid met geschriften, gegevens en biometrische kenmerken, zoals omschreven in artikel 226 eerste lid onderdelen 2° t/m 5°, 231 eerste lid, 231a eerste lid, 232 eerste lid, 310, 311, 312, 317, 321 of 326 Sr, voor zover deze feiten betrekking hebben op de verkrijging van een niet-contant betaalinstrument.

- *Diefstal (artikel 310 Sr);*

  Het wegnemen van enig goed dat geheel of ten dele toebehoort aan een ander, met het oogmerk om het zich wederrechtelijk toe te eigenen.

- *Diefstal met braak (artikel 311 Sr);*

  Het plegen van bepaalde vormen van diefstal, waaronder diefstal waarbij toegang verkregen is tot de plaats van het misdrijf door middel van valse sleutels, een valse order of het aannemen van een valse naam of hoedanigheid, of door listige kunstgrepen of door een samenweefsel van verdichtsels.

- *Verduistering (artikel 321 en 322 Sr)*

  Het opzettelijk wederrechtelijk toe-eigenen van een goed dat geheel of ten dele aan een ander toebehoort en dat iemand anders dan door misdrijf onder zich heeft. Een verhoging van de strafbedreiging volgt indien het feit begaan wordt door iemand die het goed uit hoofde van zijn persoonlijke dienstbetrekking of beroep onder zich heeft.

- *Oplichting (artikel 326 Sr);*

  Het met het oogmerk om zichzelf of een ander wederrechtelijk te bevoordelen, iemand bewegen tot de afgifte van enig goed, het verlenen van een dienst, het ter beschikking stellen van gegevens of het aangaan van een schuld, door een valse naam of van valse hoedanigheid aan te nemen, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels.

- *Flessentrekkerij (artikel 326a Sr);*

  Het tot een beroep of gewoonte maken van het kopen van goederen met het oogmerk om zonder volledige betaling zich of een ander de beschikking over die goederen te verzekeren.

- *Online handelsfraude (artikel 326e Sr);*

  Het tot een beroep of gewoonte maken van het door middel van een geautomatiseerd werk verkopen van goederen of verlenen van diensten tegen betaling met het oogmerk om zonder volledige levering zichzelf of een ander van die betaling te verzekeren.

- *Opzettelijke manipulatie computergegevens (artikel 350a Sr);*

  Het opzettelijk en wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van, dan wel het toevoegen aan, gegevens die door middel van een geautomatiseerd werk of een middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen. Ook valt hieronder het opzettelijk en wederrechtelijk verspreiden of ter beschikking stellen van gegevens die zijn bestemd om schade aan te richten in een geautomatiseerd werk.

- *Witwassen (artikel 420bis e.v. Sr).*

  Het verbergen of verhullen van de werkelijke aard, herkomst, vindplaats, vervreemding of verplaatsing van een voorwerp, dan wel het verbergen of verhullen van wie de rechthebbende op een voorwerp is of het voorhanden hebben daarvan, terwijl diegene weet dat het voorwerp onmiddellijk of middellijk afkomstig is uit enig misdrijf. Ook kwalificeert het verwerven, voor handen hebben, overdragen of omzetten van een voorwerp, dan wel gebruikmaken daarvan, terwijl diegene weet dat het voorwerp onmiddellijk of middellijk afkomstig is uit enig misdrijf.

Onder het huidige Wetboek van Strafvordering zijn deze delicten strafbare feiten waarvoor voorlopige hechtenis is toegelaten (VH-feiten). Voor de inzet van meer ingrijpende opsporingsbevoegdheden vormt het vereiste dat sprake is van een VH-feit een belangrijk drempelcriterium voor de inzet van die bevoegdheden. Welke feiten kwalificeren als VH-feit is opgenomen in artikel 67 lid 1 Sv. Onder het nieuwe Wetboek van Strafvordering is voor een andere wettelijke constructie gekozen, waarbij een verdenking van een misdrijf waarop een gevangenisstraf van vier jaar of meer is gesteld als verdenkingscriterium wordt gehanteerd. In artikel 2.1.8 nieuw Wetboek van Strafvordering is daarnaast een lijst opgenomen met feiten die met dit verdenkingscriterium gelijk worden gesteld.[29] Voor bovenstaand overzicht heeft deze wijziging geen gevolgen; ook onder het nieuwe Wetboek van Strafvordering voldoen zij aan het verdenkingscriterium.

[29] *Kamerstukken II* 2022/23, 366327, 3, p. 364.

3. Opsporing onder het huidige Wetboek van Strafvordering

In deze paragraaf bespreken we de volgende (soorten) digitale opsporingsbevoegdheden die het meest relevant (kunnen) zijn voor het opsporen van onlinefraude: (1) vorderen van identificerende en verkeersgegevens, (2) doorzoeking van geautomatiseerde werken, (3) netwerkzoeking, (4) aftappen van communicatie, en (5) hackbevoegdheid. Andere bevoegdheden uit het Wetboek van Strafvordering, zoals stelselmatige observatie (artikel 126g Sv), kunnen ook worden gebruikt, maar zijn in dit kader minder relevant en worden daarom niet besproken.[30] Aan het eind van deze paragraaf bespreken we voorts nog een bevoegdheid die belangrijk is bij de bestrijding van onlinefraude, namelijk (6) het ontoegankelijk maken van gegevens.

3.1. Vorderen van identificerende en verkeersgegevens

Aan het begin van het opsporingsonderzoek, wanneer een verdachte nog moet worden geïdentificeerd, is het vorderen van gebruikers- en identificerende gegevens van cruciaal belang. De praktijk wijst uit dat in deze fase vaak alleen een IP-adres, een bankrekening of een telefoonnummer beschikbaar is.[31] In het huidige Wetboek van Strafvordering (Sv) bestaan er twee aparte, maar vergelijkbare wettelijke regimes voor het vorderen van gegevens: één voor de vordering aan aanbieders van elektronische communicatiediensten[32] (communicatie-regime) en één voor de vordering aan andere geadresseerden (algemeen regime). Wanneer er een IP-adres of een telefoonnummer beschikbaar is, is het communicatieregime van toepassing. Op basis van deze gegevens kunnen vervolgens gebruikersgegevens, zoals naam, adres, postcode of type dienst, worden gevorderd door een opsporingsambtenaar, indien sprake is van een verdenking van een misdrijf (artikel 126na Sv). Indien bankgegevens beschikbaar zijn zal het algemene regime moeten worden gevolgd, waarbij identificerende gegevens (naam, adres, woonplaats, geboortedatum, geslacht, klant- en bankrekeningnummers) eveneens door een opsporingsambtenaar in geval van een verdenking van een misdrijf kunnen worden gevorderd (artikel 126nc Sv). In beide regimes wordt het vorderen van gebruikers- of identificerende gegevens gezien als een geringe inbreuk op de privacy, waardoor de bevoegdheid door een opsporingsambtenaar kan worden uitgeoefend. De bevoegdheidsuitoefening heeft immers enkel tot doel de identiteit van een mogelijke verdachte vast te stellen.

Onlinefraude kan ook vanuit het buitenland worden gepleegd. De hiervoor beschreven regelingen voor het vorderen van gegevens is echter niet van toepassing wanneer gegevens gevorderd moeten worden bij buitenlandse communicatieproviders, banken of andere bedrijven en personen. In dat geval kan worden verzocht om vrijwillige verstrekking van gegevens en, als dat niet lukt, moet de procedure van wederzijdse rechtshulp worden gevolgd. Om grensoverschrijdende vordering van gegevens te vereenvoudigen, kan vanaf augustus 2026 op basis van de eEvidence Verordening een verstrekkingsbevel worden uitgevaardigd.[33] Op basis van het Europees verstrekkingsbevel kunnen de bevoegde autoriteiten in een lidstaat gegevens rechtstreeks vorderen van (de wettelijke vertegenwoordiger van) een dienstverlener van de informatiemaatschappij[34] in een andere lidstaat. Dit geldt voor alle dienstverleners die hun diensten in de EU aanbieden en een substantiële connectie met een lidstaat hebben op basis van specifieke objectieve criteria, zoals een aanzienlijk aantal gebruikers of gerichtheid op een of meer lidstaten door het gebruik van de taal van die lidstaat of lidstaten. Deze dienstverleners hoeven in de EU daarom niet fysiek aanwezig te zijn. Op basis van dit

[30] Zie voor een volledig overzicht van de toepasselijke opsporingsbevoegdheden evenwel bijlage 1 – Toepasselijke opsporingsbevoegdheden onder het huidige Wetboek van Strafvordering.

[31] Zie bijvoorbeeld de volgende nieuwsberichten van het OM: https://www.om.nl/actueel/nieuws/2023/11/07/oplichting-via-1-cent-tikkies-om-eist-24-maanden-en-boete; https://www.om.nl/actueel/nieuws/2022/10/25/man24-die-valse-anwb-betalingsherinneringen-verstuurde-krijgt-drie-jaar-celstraf; https://www.om.nl/actueel/nieuws/2024/08/26/om-eist-drie-jaar-gevangenisstraf-wegens-omvangrijke-creditcardfraude; https://www.om.nl/actueel/nieuws/2019/09/24/om-eist-tot-24-maanden-gevangenisstraf-tegen-jongeren-voor-oplichting-via-marktplaats. https://www.om.nl/actueel/nieuws/2021/04/07/tot-twee-jaar-cel-geeist-voor-vriend-in-nood-fraude-via-whatsapp.

[32] Artikel 138g Sv biedt een definitie van 'aanbieders van elektronische communicatiediensten': 'De natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.' Onder deze definitie vallen bijv. openbare telecommunicatie, VPN-diensten, internet-toegangsaanbieders, interne netwerken van bedrijven of instellingen en, volgens jurisprudentie, ook hosting bedrijven en Cloud-dienstverleners.

[33] Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure, *PbEU* L 2023/191.

[34] De Verordening gebruikt de term ‘diensten van de informatiemaatschappij’ die breder is dan communicatiediensten. Deze term bevat alle elektronische communicatiediensten, opslag diensten, diensten voor internetdomeinnamen en IP-nummers.

wettelijk regime kunnen gebruikersgegevens worden gevorderd door een rechtelijke instantie of de officier van justitie (artikel 4 lid 1 onder a van de Verordening) of een opsporingsambtenaar; in het laatste geval moet het bevel worden bekrachtigd door een rechtelijke instantie of de OvJ (artikel 4 lid 1 onder b van de Verordening) Verordening). Dat betekent dat bij het vorderen van gebruikers- en identificerende gegevens, dat volgens Nederlands recht door een opsporingsambtenaar kan worden gedaan, nog een bekrachtiging van een rechtelijke instantie of officier van justitie nodig is voor een Europees verstrekkingsbevel.

Nadat de verdachte op basis van gebruikers- of identificerende gegevens is geïdentificeerd, worden vaak nog verkeers- en locatie gegevens gevorderd. Deze gegevens geven zicht op bepaalde gebeurtenissen en op het gedrag of het patroon van gedragingen van een persoon, waardoor een veel grotere inbreuk op het recht op privacy wordt gemaakt dan bij gebruikers- en identificerende gegevens. Volgens het communicatieregime kunnen verkeersgegevens (bijv. de tijd, duur, gebruikte apparatuur, afgenomen diensten en de locatie van de apparatuur) worden gevorderd door een officier van justitie in geval van VH-feiten[35] (artikel 126n Sv). Echter, op basis van jurisprudentie van het Hof van Justitie van de EU (HvJ EU) inzake de Richtlijn 2002/58/EG besliste de Hoge Raad in 2022 dat gezien de ernstige inbreuk op privacy bij het vorderen van verkeersgegevens toch een machtiging van de Rechter-Commissaris (R-C) nodig is, ook al schrijft de wet dat niet voor.[36] Omdat verkeersgegevens bijzonder vluchtig zijn (d.w.z. vatbaar voor verlies of wijziging), kan bij VH-feiten die een ernstige inbreuk op de rechtsorde opleveren ook een bevriezingsbevel worden gegeven als het onderzoek dit dringend vordert (artikel 126ni Sv). Volgens het nieuw Europese regime in de eEvidence Verordening is een grensoverschrijdend bevriezingsbevel aan een internetdienstverlener ook mogelijk (in de Verordening een 'bewaringsbevel' genoemd). Dit mag zowel door een R-C als een officier van justitie worden uitgevaardigd (artikel 4 sub 3 onder a van de Verordening); als het bevel door een opsporingsambtenaar wordt uitgevaardigd, moet deze nog door een R-C of officier van justitie worden bekrachtigd (artikel 4 sub 3 onder b van de Verordening).

In geval van een verdenking van een VH-feit kunnen volgens het algemene regime gegevens over diensten die verleend zijn (bijv. de duur, plaats en aard van de dienstverlening en profiel- of betalingsgegevens) wel worden gevorderd door een officier van justitie (artikel 126nd Sv). Dit regime valt immers niet onder de Richtlijn 2002/58/EG valt; (artikel 126nd Sv); in geval van minder ernstige misdrijven is evenwel een machtiging van de R-C vereist (artikel 126nd lid 6 Sv).

3.2. Doorzoeking van computer, smartphone of een ander geautomatiseerd werk

Omdat onlinefraude met behulp van computers, smartphones of andere geautomatiseerde werken (bijv. servers, routers, slimme apparaten) wordt gepleegd, moeten deze hulpmiddelen ook kunnen worden onderzocht. Doorzoeking van een computer, smartphone of een ander geautomatiseerd werk (hierna: computer)[37] is mogelijk op basis van twee opsporingsbevoegdheden: de doorzoeking ter inbeslagneming en de doorzoeking ter vastlegging van gegevens. Bij de 'klassieke' doorzoeking ter inbeslagneming, kunnen tijdens de doorzoeking van een plaats of voertuig ook aangetroffen computers worden onderzocht en relevante gegevens gekopieerd. Afhankelijk van de plaats die wordt doorzocht, vindt de doorzoeking zijn grondslag in verschillende artikelen die eigen voorwaarden voor de toepassing kennen (bijv. artikel 96c jo. 218, 110, 97 en 96b Sv). Zo is bijvoorbeeld de doorzoeking van een woning, waarbij een verregaande inbreuk wordt gemaakt op het recht op privacy en meer specifiek het huisrecht met de hoogste waarborgen omkleed, waarbij een machtiging van de Rechter-Commissaris vereist is (artikel 110 Sv). Alle andere plaatsen kunnen bij een verdenking van VH-feiten of in geval van ontdekking op heterdaad op basis van een bevel van de officier van justitie worden doorzocht (artikel 96c jo. 218 Sv). Voertuigen met uitzondering van woninggedeelten kunnen bij verdenking van VH-feiten of in geval van heterdaad worden doorzocht door een opsporingsambtenaar (artikel 96b Sv). Als justitie een computer alleen wil doorzoeken en gegevens wil kopiëren maar geen fysieke computer in beslag wil nemen (wat in bepaalde gevallen niet noodzakelijk en niet praktisch is), dan kan van de bevoegdheid van doorzoeking ter vastlegging van gegevens gebruik worden gemaakt (artikel 125i Sv). Deze bevoegdheid kan onder dezelfde

[35] Dit betreft strafbare feiten waarop ten minste vier jaar gevangenisstraf op staan (artikel 67 lid 1 onder a Sv), of die zijn vermeld in een van de uitzonderingsgronden (artikel 67 lid 1 onder b en c Sv). Zie ook hiervoor onder § 2.

[36] HR 5 april 2022, ECLI:NL:HR:2022:475.

[37] Artikel 80sexies Sr: 'een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken.' onder deze definitie vallen naast computers en smartphones ook modems, routers, servers, harde schrijven, USB-sticks en slimmer apparaten (indien verbonden aan een netwerk).

voorwaarden als doorzoeking ter inbeslagneming worden toegepast. Met deze bevoegdheden kunnen alleen gegevens worden doorzocht die op de computer zijn opgeslagen. Om onderzoek te doen naar gegevens die niet zijn opgeslagen op een computer maar nog in transit zijn (stromende gegevens) kan de tapbevoegdheid worden gebruikt (zie daarover nader § 3.4).

3.3. Netwerkzoeking tijdens het doorzoeken van plaatsen

Vandaag de dag zijn de meeste gegevens niet op de computer of smartphone zelf maar ergens elders opgeslagen, zoals in de Cloud,[38] op een bedrijfsserver of op andere computers die zijn aangesloten op een netwerk. Om toegang te krijgen tot deze gegevens moet gebruik worden gemaakt van een afzonderlijke bevoegdheid: onderzoek in een geautomatiseerd werk dat zich elders bevindt oftewel de netwerkzoeking. Op basis van artikel 125j Sv kunnen in geval van een doorzoeking ter vastlegging van gegevens (artikel 125i Sv) alle gegevens worden doorzocht die vanaf de doorzochte computer toegankelijk zijn maar ergens elders zijn opgeslagen (bijv. in de Cloud). Volgens artikel 125j lid 1 Sv mag dit echter alleen vanaf de plaats waar de originele doorzoeking plaatsvindt.

De netwerkzoeking heeft vaak een grensoverschrijdend karakter, zeker als het om Cloud opslag gaat. Het is immers vaak onbekend waar de servers waarop de gegevens opgeslagen zijn zich bevinden. Deze bevoegdheid is zoals alle andere opsporingsbevoegdheden in principe beperkt tot de landsgrenzen. Als het bekend is dat de server in een ander land ligt is een rechtshulpverzoek in principe het uitgangspunt. Wel is het op basis van artikel 32 onder b Cybercrimeverdrag (jo artikel 359a Sv) mogelijk om met de instemming van de communicatiedienstverlener een netwerkzoeking te verrichten naar gegevens die in een server in buitenland zijn opgeslagen. Indien de locatie van de gegevens niet bekend is (en ook niet met een redelijke inspanning te achterhalen is) mag de netwerkzoeking worden verricht ongeacht de locatie waar de gegevens zich bevinden.

3.4. Tapbevoegdheid

Het aftappen van communicatie, ook wel bekend als de tapbevoegdheid, maakt het mogelijk om communicatie af te tappen. Deze bijzondere bevoegdheid is neergelegd in artikel 126m Sv onder Titel IVa van het Eerste Boek van het Wetboek van Strafvordering. Dit betreft een ingrijpende bevoegdheid die alleen kan worden ingezet in geval van VH-feiten, die een ernstige inbreuk op de rechtsorde opleveren (artikel 126m lid 1 Sv). Niet elk geval van onlinefraude zal een ernstige inbreuk op de rechtsorde opleveren, maar gevallen van omvangrijke ernstige onlinefraude naar alle waarschijnlijkheid wel. De officier van justitie kan daartoe bevelen wanneer hij daarvoor een schriftelijke machtiging van de R-C heeft verkregen (lid 5). Zowel open als besloten telecommunicatie kan worden afgetapt, maar de plicht om mee te werken aan een tapbevel geldt alleen voor open communicatiediensten, zoals internet- en telefonieaanbieders (artikel 126m, lid 3 Sv; artikel 13.2 Tw). Besloten en andere communicatiediensten (bijv. interne netwerken van bedrijven, instellingen, ministeries, universiteiten, over-the-top communicatiediensten) hebben geen verplichting tot het verlenen van medewerking aan het tapbevel, maar zij kunnen wel vrijwillig meewerken (artikel 126m, lid 4).

Op basis van het EU Verdrag betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie (2000)[39] is grensoverschrijdend aftappen van telecommunicatie ook mogelijk (artikel 20 Verdrag). De OvJ moet wel na de afgifte van het bevel tot aftappen eerst de andere verdragsstaat in kennis stellen en om toestemming vragen (artikel 126ma lid 1 Sv). De bevoegdheid om direct af te luisteren (artikel 126l Sv) kan ook worden ingezet, waarbij vertrouwelijke communicatie kan worden opgenomen met een technisch hulpmiddel (bijv. een richtmicrofoon of keylogger). Onder vertrouwelijke communicatie wordt verstaan de uitwisseling van berichten tussen personen die in beslotenheid plaatsvindt, bijvoorbeeld een in beslotenheid gevoerd gesprek of een niet-openbaar e-mailbericht. Net zoals bij de tapbevoegdheid kan deze bevoegdheid alleen worden ingezet bij de verdenking van VH-feiten, die een ernstige inbreuk op de rechtsorde opleveren (lid 1) en na een machtiging van de R-C (lid 4).

3.5. Hackbevoegdheid

De recent geïntroduceerde mogelijkheid tot onderzoek in een geautomatiseerd werk, beter bekend als de hackbevoegdheid, leidt ook tot elektronisch bewijs. Met deze bevoegdheid, beschreven in de

[38] Denk bijvoorbeeld over Dropbox, iCloud, Picasa en Google Drive diensten.

[39] Overeenkomst, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie, betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, *PbEU* C 2000/197.

artikelen 126nba en 126uba (criminele organisatie) Sv, kreeg de politie de mogelijkheid om zich heimelijk en op afstand toegang verschaffen tot een geautomatiseerd werk met behulp van een technisch hulpmiddel (d.w.z. malware, waarbij kwetsbaarheden worden gebruikt om bij computers van verdachten binnen te komen). Bij deze bevoegdheid is sprake van een zeer grote inbreuk op privacy. De hackbevoegdheid vormt een paraplubegrip waaronder een aantal ingrijpende opsporingsmodaliteiten vallen: het vaststellen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker (artikel 126nba lid 1 onder a Sv), het opnemen van communicatie artikel 126nba lid 1 onder b Sv), het stelselmatig observeren van gedrag van een persoon met een technisch hulpmiddel (artikel 126nba lid 1 onder cv Sv), het vastleggen van (huidige of toekomstige) gegevens in een computer (artikel 126nba lid 1 onder d Sv), en ontoegankelijk maken van gegevens (artikel 126nba lid 1 onder e Sv). Daardoor wordt de hackbevoegdheid ook wel gezien als de meest verregaande en ingrijpende bevoegdheid voor het recht op privacy, waardoor deze alleen in uitzonderlijke gevallen mag worden gebruikt (eisen van subsidiariteit en proportionaliteit).

Deze bevoegdheid is daarom ook met uitzonderlijk veel voorwaarden en waarborgen omkleed (niet alleen in de wetsartikelen zelf maar ook bij algemene maatregel van bestuur). Om gebruik te maken van bevoegdheden zoals omschreven in 126nb lid 1 onder a-c Sv is een bevel van de officier van justitie na een schriftelijke machtiging van de R-C nodig. Voorts kan de bevoegdheid enkel worden ingezet in geval van een verdenking van een VH-feit die de rechtsorde ernstig schaadt en voor zover dat strikt noodzakelijk is (artikel 126nba lid 1). Naast de officier van justitie en de R-C maakt ook de Centrale Toetsingscommissie een afweging of de inzet van de bevoegdheid proportioneel en subsidiair is. Verder kunnen de bevoegdheden onder d en e (online doorzoeking en ontoegankelijk maken van gegevens) alleen worden gebruikt bij misdrijven die worden bedreigd met een gevangenisstraf van maximaal 8 jaar of meer en misdrijven die bij Algemene Maatregel van Bestuur worden aangewezen (bijv. gebruik van botnets, grooming, bommeldingen en witwassen). Bij onlinefraude voor zover deze zo ernstig is dat het een ernstige inbreuk op de rechtsorde oplevert zijn vaak alleen de functionaliteiten van a-c van toepassing. Echter, de bevoegdheidsuitoefening moet ook strikt noodzakelijk en proportioneel zijn. Gezien alle andere bevoegdheden die beschikbaar zijn om onlinefraude op te sporen, is het niet aannemelijk dat het gebruik van de hackbevoegdheid proportioneel en subsidiair kan worden geacht om onlinefraude te bestrijden. Bovendien laat de praktijk zien dat door de strenge voorwaarden voor de inzet van deze bevoegdheid van de hackbevoegdheid maar weinig gebruik wordt gemaakt: slechts dertig keer in 2023.[40]

3.6. Ontoegankelijk maken van gegevens

Bij onlinefraude waarbij malware en phishingwebsites vaak worden gebruikt zijn twee bevoegdheden om gegevens ontoegankelijk te maken van groot belang. Ten eerste kan gebruik worden gemaakt van de bevoegdheid om gegevens ontoegankelijk te maken (artikel 125o Sv). Deze bevoegdheid is van toepassing op situaties waarin bij een doorzoeking van een computer (zie sectie 3.2) onrechtmatige gegevens worden aangetroffen. Met ‘onrechtmatige gegevens’ worden gegevens bedoeld ‘die naar hun aard niet in het normale, legale verkeer aanwezig behoren te zijn, althans niet in de beschikkingsmacht van personen met kwade bedoelingen’.[41] Voorts moet er een zeker verband bestaan tussen de onrechtmatige gegevens en een strafbaar feit: het moeten gegevens zijn met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd. Ook moet de maatregel noodzakelijk zijn ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Hieronder valt dan ook malware waarmee onlinefraude is of kan worden gepleegd. Op basis van deze bevoegdheid kan de officier van justitie (soms na een machtiging van de R-C, afhankelijk van de plaats dat wordt doorzocht (zie § 3.2)) bevelen dat deze malware wordt verwijderd of op een andere wijze ontoegankelijk wordt gemaakt (lid 2). Voor de keuze van de juiste maatregel moet gekeken worden naar de effectiviteit in een concrete situatie, rekening houdend met de eisen van proportionaliteit en subsidiariteit.[42]

Als laatst is nog de zogenoemde *notice-and-takedown* (NTD) bevoegdheid van belang (artikel 125p Sv). Op basis van deze bevoegdheid kan de OvJ na een machtiging van de R-C bij VH-feiten een aanbieder van een communicatiedienst bevelen om een website offline te halen of gegevens die via internet worden aangeboden ontoegankelijk te maken. Hiermee wordt bereikt dat een strafbaar feit wordt beëindigd of een nieuw strafbaar feit voorkomen. De ‘notice-and-takedown’ is dan een

[40] Verslag Toezicht wettelijke hackbevoegdheid politie 2023.
[41] *Kamerstukken II* 1998/99, 26671, 3, p. 20.
[42] *Kamerstukken II* 1998/99, 26 671, 3, p. 21.

procedure waarbij een partij in kennis wordt gesteld (de 'notice') van onmiskenbaar onrechtmatig of strafbaar materiaal op een onlinebron met verzoek dit materiaal te verwijderen (de takedown). Het bevel wordt pas ingezet als de aanbieder geen opvolging geeft aan de vrijwillige NTD-gedragscode of niet bij deze code is aangesloten.[43]

4. Opsporing onder het nieuwe Wetboek van Strafvordering

4.1. Algemeen

Onder het nieuwe Wetboek van Strafvordering wordt de regeling voor digitale opsporing volledig geherstructureerd, waarbij het onderzoek van gegevens een centrale positie krijgt.[44] In dat kader is in het bijzonder Hoofdstuk 7, Titel 7.3 Onderzoek van gegevens en Hoofdstuk 8 Heimelijk bevoegdheden van Boek 2 van belang. Met het oog op de toekomstbestendigheid en flexibiliteit van het nieuwe Wetboek van Strafvordering, zijn de bevoegdheden zoveel mogelijk techniekonafhankelijk geformuleerd.[45] Voor de opsporing van onlinefraude zijn in het bijzonder de nieuw te introduceren opsporingsbevoegdheden het kennisnemen van gegevens na inbeslagname (artikel 556 Sv en artikel 2.7.39 nieuw Wetboek van Strafvordering), de netwerkzoeking na inbeslagname (artikel 557 Sv en artikel 2.7.40 nieuw Wetboek van Strafvordering), het bevel data-analyse door een derde (artikel 2.7.50 nieuw Wetboek van Strafvordering) en de stelselmatige locatiebepaling van belang (artikel 2.8.18 nieuw Wetboek van Strafvordering). Met het kennisnemen van gegevens na inbeslagname en de netwerkzoeking na inbeslagname is reeds ervaring opgedaan onder de Innovatiewet Strafvordering[46].

De basis voor de normering van het onderzoek aan gegevens vindt zijn grondslag in het rapport van de Commissie Koops inzake de regulering van opsporingsbevoegdheden in een digitale omgeving.[47] Het uitgangspunt is daarbij wanneer de inbreuk op bepaalde grondrechten, waaronder in het bijzonder de persoonlijke levenssfeer van personen, groter is, de regeling voor de toepassing van bevoegdheden preciezer moet zijn geformuleerd en hoe hoger de functionaris is die de toepassing van de bevoegdheid moet goedkeuren. Dat betekent dus dat indien er geen of een beperkte inbreuk wordt gemaakt op de grondrechten van burgers én er geen sprake is van een risico voor de integriteit en beheersbaarheid van de opsporing een algemene bevoegdheid tot opsporing volstaat.[48] De bevoegdheid kan in dat geval worden uitgeoefend door een opsporingsambtenaar. Is echter sprake van een meer dan een geringe inbreuk op de grondrechten van burgers of is de inzet van de opsporingsbevoegdheid risicovol voor de integriteit en beheersbaarheid van de opsporing, dan dient er een specifieke wettelijke grondslag te zijn en dient de (hulp-)officier tot de inzet van de bevoegdheid te bevelen, al dan niet met machtiging van de Rechter-Commissaris (R-C).[49] De grootte van de inbreuk op de persoonlijke levenssfeer wordt aldus bepaald aan de hand van het stelselmatigheidscriterium. Voor de beoordeling kan in dat kader worden gekeken naar een samenstel van factoren, zoals de hoeveelheid, de aard en wijze van (geautomatiseerd) onderzoek van de gegevens, type gegevensdrager en de wijze van opslag.[50]

4.2. Nieuwe bevoegdheden onder de Innovatiewet

4.2.1. Kennisnemen gegevens na inbeslagname

Met de Innovatiewet Strafvordering werd reeds ervaring opgedaan met de nieuwe bevoegdheid geïntroduceerd voor het kennisnemen van gegevens die na inbeslagneming 'binnenkomen' op een computer en die ingezet kan worden bij ontdekking op heterdaad of in geval van een verdenking van

[43] Zie hierover uitgebreider *Kamerstukken II* 2008/09, 28684, 232.

[44] Zie voor een uitgebreide analyse L. Stevens & M.I. Fedorova, *Inhoudelijke rapportage Boek 2: Het* opsporingsonderzoek, 11 september 2023. Gepubliceerd als Kamerstuk van de Tweede Kamer: *Kamerstukken II*, 36327, p. 53 e.v.

[45] Kamerstukken II 2022/23, 36 327, 3, p. 337. Stevens & Fedorova 2023 (vnt. 44), p. 6.

[46] *Stb*. 2022, 276.

[47] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.

[48] Stevens & Fedorova 2023 (vnt. 44), p. 54. De toepasselijke bepaling is in dat geval artikel 2.1.9 nieuw Wetboek van Strafvordering.

[49] Stevens & Fedorova 2023 (vnt. 44), p. 54

[50] Kamerstukken II 2022/23, 36 327, 3, p. 573. Stevens & Fedorova 2023 (vnt. 44), p. 54.

een VH-feit (artikel 556 Sv).[51] Onder het nieuwe Wetboek van Strafvordering wordt deze regeling opgenomen in artikel 2.7.39.

In de praktijk zal het onderzoek aan de gegevens dikwijls niet direct na de inbeslagname van een apparaat van start gaan, omdat in veel gevallen eerst de beveiliging moet worden doorbroken of omdat er meerdere apparaten in beslag zijn genomen,[52] waarbij eerst moet worden bepaald welk van de apparaten moet worden onderzocht en welk type onderzoek nodig is.[53] Het eerste lid van artikel 556 Sv ziet daarom op het kennisnemen van gegevens die gedurende de eerste drie dagen na de inbeslagneming van de computer worden opgeslagen. Daarvoor is een machtiging van de R-C voor het bevel van de officier van justitie vereist. Indien het belang van het onderzoek dit dringend vordert, mag ook kennis worden genomen van gegevens die gedurende in totaal zes maanden na de inbeslagneming op de computer worden opgeslagen. Ook in dat geval is een machtiging van de R-C voor het bevel van de officier van justitie vereist (artikel 556 lid 2 en 3 Sv).[54]

Uit de evaluatie Innovatiewet Strafvordering in 2024 is gebleken dat deze bevoegdheid in het algemeen een verbetering van de strafvordering oplevert.[55] Wel is geconstateerd dat er geen behoefte is om een afzonderlijke bevoegdheid te creëren voor onderzoek naar gegevens die na inbeslagneming zijn opgeslagen op het apparaat. In plaats daarvan wordt het wenselijk geacht dat de mogelijkheid om 'nieuwe gegevens' te doorzoeken deel uitmaakt van de algemene bevoegdheid om gegevens te onderzoeken.[56] Daarmee zou ook de kritiek op de gestelde termijnen waarbinnen de gegevens mogen worden onderzocht worden ondervangen.[57]

4.2.2. Netwerkzoeking na inbeslagname

Het vereiste om de netwerkzoeking in verband met de doorzoeking (volgens artikel 125i) en vanaf de plaats van de doorzoeking te verrichten werd in de praktijk als een groot knelpunt ervaren (zie hiervoor in par. 3.3).[58] Onder de Innovatiewet Strafvordering werd daarom bezien of een nieuwe, aanvullende regeling voor de netwerkzoeking in artikel 557 Sv een oplossing voor die problematiek zou bieden. Deze bepaling is in het nieuwe Wetboek van Strafvordering opgenomen in artikel 2.7.40.

De nieuwe bevoegdheid tot netwerkzoeking na inbeslagname is een zelfstandige bevoegdheid die betrekking heeft op hetzelfde onderwerp als artikel 125j Sv, maar onder andere omstandigheden wordt uitgeoefend: namelijk kennisneming na inbeslagneming, in plaats van tijdens een doorzoeking. Deze bevoegdheid vereist dat er een machtiging door de R-C is afgegeven voor het bevel van de officier van justitie (artikel 557 lid 1 Sv). Op basis van artikel 557 Sv kan de netwerkzoeking op het politiebureau worden verricht en is het ook los van de context van een doorzoeking ter vastlegging van gegevens mogelijk (bijv. in gevallen waarin een smartphone tijdens een aanhouding inbeslaggenomen werd). Op basis van deze bevoegdheid kunnen ook gegevens worden doorzocht die na de inbeslagneming elders binnenkomen. Het eerste lid van artikel 557 Sv ziet op het kennisnemen van gegevens die gedurende de eerste drie dagen na de inbeslagneming worden opgeslagen. Dit is mogelijk in geval van ontdekking op heterdaad of bij VH-feiten waarvoor een met machtiging van de R-C vereist is. Het tweede en derde lid maken het mogelijk om kennis te nemen van gegevens die in totaal zes maanden na de inbeslagneming worden opgeslagen. Deze bevoegdheid mag alleen worden gebruikt indien het belang van het onderzoek dit dringend vordert en op basis van een machtiging van de R-C.

Uit de evaluatie Innovatiewet Strafvordering in 2024 is gebleken dat ook deze bevoegdheid in het algemeen een verbetering van de strafvordering oplevert. Wel zijn een aantal belangrijke knelpunten geconstateerd. Ten eerste is gebleken dat het regime van lid 1 met de termijn van drie dagen (gerekend vanaf het moment van inbeslagneming) vaak niet voldoende is voor het uitoefenen van

[51] B. de Wilde, M. Boiten, M. Hanswijk, S. Stone en T. van der Vorst, *Evaluatie Innovatiewet Strafvordering, Pilots Gegevens na beslag, Audiovisuele registratie en Hulpofficier van Justitie*, Den Haag: WODC 2024, p. 47.

[52] In dat kader is ook artikel 558 Sv relevant, wat het mogelijk maakt onder dwang van de verdachte de biometrische beveiliging te doorbreken. Overigens is volgens de jurisprudentie van de Hoge Raad momenteel ook al mogelijk om in bepaalde gevallen de biometrische beveiliging te doorbreken. Zie daarover HR 9 februari 2021, ECLI:NL:HR:2021:202, NJ 2021/120. Zie eveneens De Wilde e.a. 2024 (vnt. 51), p. 43.

[53] De Wilde e.a. 2024 (vnt. 51), p. 48.

[54] Deze wordt steeds gegeven voor een periode van maximaal 3 maanden.

[55] De Wilde e.a. 2024 (vnt. 51), p. 68.

[56] De Wilde e.a. 2024 (vnt. 51), p. 75.

[57] De Wilde e.a. 2024 (vnt. 51), p. 68: In de praktijk blijkt een periode van drie dagen vaak niet te volstaan voor de toepassing van artikel 556 Sv. Dit heeft onder meer te maken met de te volgen procedure, onduidelijkheid over het onderscheid tussen onderzoek met een onderzoeksbelang en dringende noodzakelijkheid. In sommige gevallen bleek ook de termijn van 6 maanden te kort te zijn, bijvoorbeeld wanneer sprake was van een goede beveiliging op het apparaat.

[58] Het rapport van de Commissie Koops.

deze bevoegdheid, waardoor gebruik moet worden gemaakt van het regime in lid 2 met de maximale termijn van zes maanden.[59] Het tweede knelpunt heeft te maken met het vereiste dat op grond van artikel 557 Sv alleen gegevens mogen worden vastgelegd die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Volgens het rapport is een selectie van alleen relevante gegevens technisch niet mogelijk. In de praktijk worden daarom veel of alle gegevens vastgelegd die niet relevant zijn voor het onderzoek waarvan dan een rest-proces-verbaal wordt opgemaakt.[60]

4.3. Nieuw te introduceren opsporingsbevoegdheden

4.3.1. Bevel data-analyse door een derde

Een nieuwe vorm van elektronisch bewijs zijn de resultaten uit een data-analyse door een derde. Onder het nieuwe Wetboek van Strafvordering wordt deze mogelijkheid neergelegd in artikel 2.7.50. Daarmee is gehoor gegeven aan de aanbevelingen van de Commissie Mevis, en meer recent de Commissie Koops.[61] Het bevel data-analyse door een derde maakt het mogelijk voor de officier van justitie om bedrijven of instellingen, waarvan redelijkerwijs vermoed kan worden dat zij toegang hebben tot bepaalde gegevens, te bevelen dat deze gegevens worden bewerkt en de resultaten daarvan worden verstrekt aan de opsporingsautoriteiten.[62] Vereist is dat sprake is van een verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf is gesteld van vier jaar of meer. Het bevel tot data-analyse door een derde gaat verder dan het bevel tot verstrekking van gegevens: het gaat hier niet om het simpelweg opzoeken en verstrekken van gegevens. Gedacht kan worden aan het integraal vergelijken van gegevens uit de ene dataset met alle gegevens uit een andere dataset (bijvoorbeeld gegevens van verschillende malafide verkoopadvertenties van marktplaats met gegevens uit malafide verkoopadvertenties van eBay), om zo gegevens te identificeren die in beide sets voorkomen. De data-analyse levert in zoverre dus nieuwe gegevens op die vervolgens worden verstrekt.[63] Volgens de memorie van toelichting is er vanwege de grote hoeveelheid gegevens die in handen zijn van verschillende bedrijven en instellingen behoefte aan een dergelijke mogelijkheid. Bij zulke grote hoeveelheden gegevens is het lastig om de relevantie en bruikbaarheid van de gegevens te beoordelen en blijven ook gegevens bewaard die een onnodige inbreuk op de privacy van burgers maken.[64]

4.3.2. Stelselmatige locatiebepaling

Wanneer de verdachte van de onlinefraude is geïdentificeerd kan ter aanhouding van de verdachte of ter uitvoering van andere heimelijke opsporingsbevoegdheden op stelselmatige wijze de locatie van een persoon worden bepaald met behulp van een technisch hulpmiddel (artikel 2.8.18). Daarbij kan gedacht worden aan het versturen van een stille SMS, waardoor het telefoontoestel contact maakt met het telecommunicatienetwerk, waardoor de locatie van verdachte kan worden bepaald.[65] Ook de inzet van een IMSI-catcher valt hieronder, waarbij door middel van scanapparatuur een nummer van een telefoontoestel kan worden verkregen of de locatie van een persoon kan worden bepaald.[66] De bevoegdheid dient te worden ingezet als steunbevoegdheid. Dat wil zeggen dat de inzet altijd tot doel heeft om andere bevoegdheden – in dit geval de aanhouding van de verdachte of inzet van andere heimelijke bevoegdheden – mogelijk te maken. Deze bevoegdheid kent vooralsnog geen nadere normering, zoals een machtiging van de R-C, maar ontwikkelingen inzake de Unierechtelijke regeling betreffende de bescherming van persoonsgegevens kan daar in de toekomst mogelijk wel toe dwingen.[67]

---

[59] De Wilde e.a. 2024 (vnt. 51), p. 9.

[60] De Wilde e.a. 2024 (vnt. 51), p. 9.

[61] Commissie strafvorderlijk gegevensverwerking in de informatiemaatschappij (Commissie Mevis), Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, mei 2001 en Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops), Regulering van opsporingsbevoegdheden in een digitale omgeving, 2018, p. 179-187.

[62] *Kamerstukken II* 2022/23, 366327, 3, p. 610.

[63] *Kamerstukken II* 2022/23, 366327, 3, p. 612.

[64] Zie de kritische noot van de NoVA over de data-analyse en verschoningsgerechtigde informatie en de vragen van Stevens & Fedorova over de keuze om het gedifferentieerde stelsel van normering naar gelang de ingrijpendheid voor de privacy hier niet door te trekken. Zie Stevens & Fedorova 2023 (vnt. 44), p. 60.

[65] *Kamerstukken II* 2022/23, 366327, 3, p. 718.

[66] *Kamerstukken II* 2022/23, 366327, 3, p. 719.

[67] Stevens & Fedorova 2023 (vnt. 44), p. 71.

5. Conclusie en reflectie

(Online)fraude is een complex en wijdverspreid probleem dat voorkomt in alle lagen van de samenleving. Terwijl klassieke vormen van (offline) criminaliteit de afgelopen jaren afneemt, neemt het aantal gevallen van online criminaliteit alleen maar toe.[68] Ondanks dat maar weinig mensen aangifte doen van onlinefraude (in 2024 slechts 21%)[69], zijn de gevolgen van fraude omvangrijk: financiële, emotionele en psychische schade en verlies aan vertrouwen door burgers in mensen, het economisch systeem en het maatschappelijk verkeer.[70] Beleidsmakers roepen daarom al enkele jaren op tot een harde aanpak van fraudeurs.[71] Zaken als de toeslagenaffaire hebben laten zien dat dergelijk beleid daarin vaak door kan schieten en dat de menselijke maat met enige regelmaat uit het oog verloren wordt.[72] Het is daarom belangrijk om duidelijke richtlijnen te hebben voor fraudebestrijding.[73]

In deze bijdrage is een overzicht geboden van de verschillende mogelijkheden om onlinefraude op te sporen en te vervolgen. Voor de vervolging van onlinefraude biedt het Wetboek van Strafrecht verschillende mogelijkheden, zoals de strafbaarstelling computervredebreuk, oplichting, witwassen en valsheid in geschrifte. Deze delicten voldoen aan het verdenkingscriterium, waardoor het mogelijk is om ook meer ingrijpende opsporingsbevoegdheden in te zetten om de verdachten van deze strafbare feiten op te sporen.[74]

Onder het huidige Wetboek van Strafvordering zijn al een groot aantal opsporingsbevoegdheden om onlinefraude op te kunnen sporen. De belangrijkste opsporingsbevoegdheden zijn het vorderen van identificerende en verkeersgegevens, doorzoeking van geautomatiseerde werken, netwerkzoeking tijdens het doorzoeken van plaatsen, aftappen van communicatie en de hackbevoegdheid. Daarnaast zijn de bevoegdheden inzake het ontoegankelijk maken van gegevens van belang bij de bestrijding van onlinefraude.[75]

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 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.[76]

Hoewel het straf(proces)recht dus verschillende mogelijkheden bevat om onlinefraude te opsporen en te vervolgen, is uit onderzoek gebleken dat het strafrecht slechts een beperkte rol speelt bij het bestrijden van onlinefraude.[77] Opsporingsbevoegdheden zijn immers vooral gericht op strafbare feiten die al hebben plaatsgevonden (ook al zijn sommige bevoegdheden, zoals het verwijderen van gegevens meer preventief van aard). Voorts maakt het vaak aanwezige grensoverschrijdende aspect van onlinefraude de opsporing van onlinefraudeurs lastig. Door beleidsmakers is dan ook onderkend dat de aanpak van onlinefraude niet slechts een strafrechtelijke aangelegenheid is.[78] (Online) fraude kan door middel van verschillende rechtsgebieden – zoals het privaatrecht, bestuursrecht, het tuchtrecht en het strafrecht – worden aangepakt, waardoor verschillende autoriteiten en instanties, zoals AFM, de Belastingdienst, instellingen, bedrijven en burgers verantwoordelijk zijn voor de

[68] Buisman 2021 (vnt. 6), p. 359. Vgl. CBS 2024 (vnt. 3).
[69] Zie CBS 2024 (vnt. 3).
[70] Buisman 2021 (vnt. 6), p. 359. CBS 2024 (vnt. 3).
[71] Zie bijvoorbeeld *Kamerstukken II* 2014/15, 17050, nr. 496
[72] Parlementaire ondervragingscommissie Kinderopvangtoeslag, *Ongekend onrecht. Parlementaire ondervraging Kinderopvangtoeslag*, Tweede Kamer der Staten-Generaal, 17 december 2020. Vgl. Buisman 2021 (vnt. 6), p. 359
[73] Buisman 2021 (vnt. 6), p. 366.
[74] Zie nader § 2.
[75] Zie nader § 3.
[76] Zie nader § 4.
[77] Zie bijv. Jansen e.a. 2019 (vnt. 16).
[78] Zie het Actieplan Integrale aanpak online fraude 2024, te raadplegen via www.rijksoverheid.nl. Vgl. M.F.H. Hirsch Ballin, *VU Amsterdam Position paper Rondetafelgesprek 13 januari 2022 over 'CIFAS'*.

bestrijding van onlinefraude en er een verscheidenheid aan middelen en maatregelen inzake het toezicht, de opsporing en de afdoening van fraudeleuze handelingen beschikbaar is.[79]

Tot op heden is de integrale aanpak vooral praktisch ingericht: gebaseerd op vrijwillige samenwerking tussen meerdere private en publieke partijen en primair gericht op preventie. Zo wordt in Nederland aankoopfraude aangepakt door onder meer het Landelijk Meldpunt Internetoplichting (LMIO) en de Fraudehelpdesk.[80] In plaats van opsporing van al gepleegde onlinefraude ligt de focus hier op verstoringstechnieken om onlinefraude te verminderen, zoals het offline halen van frauduleuze webwinkels en advertenties (op basis van vrijwillige medewerking van online platforms en websites). De politie vraagt bijvoorbeeld bedrijven die websites in de lucht houden om een frauduleuze webwinkel offline te halen. Volgens de Consumentenbond werkt deze aanpak goed: zo'n 80% van de nepshops is binnen 5 dagen uit de lucht. Een klein deel (12%) blijft langer dan 2 weken online.[81] Om frauduleus geldverkeer te verstoren werpen ook banken een drempel op middels de IBAN-Naam Check.[82]

Met het oog op de praktische aanpak van de bestrijding van onlinefraude speelt het recht op gegevensbescherming een bijzonder belangrijke rol. Hoewel gegevensbeschermingsrecht soms wordt gezien als een obstakel in de bestrijding van onlinefraude, staat de wet de verwerking van persoonsgegevens voor dit doel toe, mits deze verwerking op een rechtmatige en legitieme manier gebeurt (d.w.z. waarbij de fundamentele rechten en vrijheden van personen worden gerespecteerd). Gegevensverwerking op het gebied van fraudepreventie kan haar rechtsgrondslag vinden in artikel 6, lid 1, onder f) AVG (Overweging 47 AVG). De Overweging 47 AVG verduidelijkt dat de verwerking van persoonsgegevens die strikt noodzakelijk is voor fraudepreventie een gerechtvaardigd belang kan vormen. De verwerking van persoonsgegevens in het legitieme belang van fraudepreventie is echter niet zonder voorwaarden en beperkingen, met name omdat deze vorm van gegevensverwerking aanzienlijke gevolgen kan hebben voor de betrokkenen. Het Europees Comité voor gegevensbescherming (*European Data Protection Board*)[83] heeft in 2024 richtsnoeren uitgegeven over de verwerking van persoonsgegevens op basis van artikel 6, lid 1, onder f), AVG, die ook een leidraad kan bieden voor de verwerking van persoonsgegevens voor fraudepreventie (niet specifiek met betrekking tot onlinefraude).[84] Deze Richtsnoeren maken duidelijk dat de verwerking "strikt noodzakelijk [moet] zijn met het oog op fraudepreventie". Of daarvan sprake is moet in samenhang met het beginsel van "gegevensminimalisering" (artikel 5, lid 1, onder c), AVG) worden onderzocht. Tegelijkertijd moet rekening worden gehouden met het beginsel van opslagbeperking in artikel 5, lid 1, onder e) AVG bij het bepalen van het beleid inzake de bewaring van gegevens, die worden verwerkt voor fraudeopsporings- of preventiedoeleinden.

Bij de afweging of sprake is van strikte noodzakelijkheid spelen verschillende afwegingen een rol. Gegevens die worden verwerkt, moeten bijvoorbeeld nauwkeurig zijn en aantoonbaar relevant om te beoordelen of een betrokkene het risico loopt het slachtoffer te worden van fraude. De voor de verwerking van de gegevens verantwoordelijke autoriteiten moeten specifiek aangeven welk type fraude ze proberen te voorkomen en welke gegevens ze noodzakelijkerwijs moeten verwerken om dat type fraude te voorkomen. Dat betekent dat gegevens alleen worden verzameld voor specifiek bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Een algemene verwijzing naar het doel van "fraudebestrijding", bijvoorbeeld in het privacybeleid, is daarom ook niet voldoende om te voldoen aan de transparantie- en documentatieverplichtingen onder de AVG.

[79] Buisman 2021 (vnt. 6), p. 359. Hirsch Ballin 2022 (vnt. 78) Zie ook het WODC-onderzoek dat wordt uitgevoerd door de Vrije Universiteit Amsterdam inzake het gebruik van interventies in de aanpak van financieel-economische criminaliteit (projectnummer 3384).
[80] Jansen e.a. 2019 (vnt. 16), p. 23.
[81] 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.
[82] Jansen e.a. 2019 (vnt. 16), p. 24.
[83] Het Comité is een onafhankelijk Europees orgaan dat erop toeziet dat de Algemene verordening gegevensbescherming consequent wordt toegepast en dat de samenwerking tussen de gegevensbeschermingsautoriteiten van de EU bevordert.
[84] European Data Protection Board, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, version 1.0*, aangenomen op 8 oktober 2024.

Deze factsheet is tot stand gekomen in het kader van de samenwerking van de Tweede Kamer met De Jonge Akademie, de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), de Nederlandse Federatie van Universitair Medische Centra (NFU), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), TNO en de Vereniging Universiteiten van Nederland (UNL).

Disclaimer

De Jonge Akademie, KNAW, NFU, TNO en UNL bemiddelen tussen parlementaire kennisvraag en wetenschappelijk kennisaanbod. De informatie in het kader van Parlement en Wetenschap is afkomstig van vooraanstaande wetenschappers, maar niet onderworpen aan peer review en niet door de wetenschaps-organisaties geverifieerd.

Bijlage 1 – Toepasselijke opsporingsbevoegdheden onder het huidige Wetboek van Strafvordering[85]

Onderzoeksbevoegdheid	Omschrijving
Inbeslagneming voorwerpen	
96 Sv	Het in beslag nemen van daarvoor vatbare voorwerpen door opsporingsambtenaar en daartoe elke plaats betreden.
96a Sv	Bevoegdheid voor opsporingsambtenaar om te bevelen dat iemand waarvan redelijkerwijs kan worden vermoed dat hij houder is van een voor beslagneming vatbaar voorwerp dit voorwerp uitlevert.
96b Sv	Doorzoeken vervoermiddel voor daarvoor vatbare voorwerpen.
96c Sv	Doorzoeken van alle plaatsen (in beginsel) door de OvJ, met uitzondering van een woning zonder toestemming van de bewoner en een kantoor van een persoon met verschoningsrecht (218, 218a Sv).
97 Sv	Doorzoeken woning van zonder toestemming bewoner door de OvJ (in beginsel) op machtiging van R-C.
110 Sv	Doorzoeken van elke plaats door de R-C ter inbeslagneming voorwerpen.
Doorzoeking ter vastlegging gegevens	
94 jo. 95 Sv en 96 Sv, in combinatie met Smartphone-arrest	Het doorzoeken van een gegevensdrager bij het in beslag nemen door opsporingsambtenaar of bij staandehouding.
125i Sv	Bevoegdheid tot het doorzoeken van een plaats en vastleggen van de gegevens die aanwezige gegevensdragers houden.
125j Sv	Bevoegdheid tot doorzoeken geautomatiseerd werk elders aanwezig.
125k Sv	Bevoegdheid tot vorderen ontsluiten van gegevensdrager of versleutelde gegevens.
125o Sv	Bevoegdheid tot ontoegankelijk maken van de gegevens met betrekking tot of behulpzaam bij het strafbare feit ontoegankelijk maken.
125p Sv	Bevoegdheid tot bevelen aanbieder communicatiedienst tot ontoegankelijk maken gegevens.
Vordering van gegevens	
Algemeen regime	
126nc Sv	Bevoegdheid tot het vorderen van persoonsgegevens door opsporingsambtenaar.

[85] Bij onderstaande tabel verdient opmerking dat gegevensdragers gezien worden als voorwerpen die voor beslagneming in aanmerking komen onder het Nederlandse recht.

	*Voor deze bevoegdheid is geen verdenking van een VH-feit vereist, enkel verdenking van een misdrijf.
126nd Sv	Bevoegdheid tot vorderen verstrekking gewone gegevens door de OvJ van opgeslagen of vastgelegde gegevens.
126nda Sv	Bevoegdheid voor de opsporingsambtenaar om beelden gemaakt met camera's voor de beveiliging van goederen, gebouwen of personen.
126ne Sv	Bevoegdheid van de OvJ tot het bepalen dat de vordering uit 126nd Sv ook ziet op gegevens die eerst na het tijdstip van de vordering worden verwerkt.
126nf Sv	Bevoegdheid voor de OvJ om, onder omstandigheden, beschermde persoonsgegevens te vorderen.
126ng Sv	Bevoegdheid om een vordering als in 126nc of 126nd Sv te richten jegens een aanbieder van een telecommunicatiedienst, indien de vordering ziet op gegevens die niet gevorderd kunnen worden volgens 126n en 126na Sv, al dan niet op voorwaarde van bijkomende omstandigheden.
126nh Sv	Bevoegdheid voor de OvJ om ontsleuteling te vorderen van degene die redelijkerwijs kan worden vermoed kennis te hebben van de wijze van versleuteling, in geval van een vordering als in 126nd, 126ne of 126nf Sv.
126ni Sv	Bevoegdheid voor de OvJ om gegevens, onder bijkomende omstandigheden, te bewaren en beschikbaar te houden (bevriezen).
Communicatieregime	
126m Sv	Bevoegdheid voor de OvJ om aan een opsporingsambtenaar, onder bijkomende omstandigheden, te bevelen dat er wordt opgenomen communicatie met gebruikmaking van de diensten van een aanbieder van een telecommunicatiedienst die niet voor het publiek bestemd is (tap).
126ma Sv	126m Sv met betrekking tot een persoon die zich in het buitenland bevindt.
126n Sv	Bevoegdheid tot het vorderen van verkeersgegevens door de OvJ.
126na Sv	Bevoegdheid tot het vorderen van bepaalde gegevens door opsporingsambtenaar van een communicatiedienst.
126nba Sv	Bevoegdheid voor de OvJ te bevelen dat een opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel onderzoek te doen (hacken).
Opnemen vertrouwelijke informatie	
126l Sv	Bevoegdheid voor de OvJ te bevelen dat een (bepaalde type) opsporingsambtenaar vertrouwelijke communicatie opneemt met een technisch hulpmiddel. Deze vertrouwelijke communicatie kan op verschillende wijzen plaatsvinden, waaronder via gesproken woord en via de kabel. Ook is het mogelijk een besloten plaats binnengetreden wordt zonder toestemming van de rechthebbende, en onder bijkomende omstandigheden, een woning zonder toestemming van de rechthebbende.
Openbare informatie	

38 Wiv 2017, 3 Polw, 126j Sv	Onderzoek doen met openbare digitale informatie (soms ook wel “open bron” genoemd)
Bijzondere opsporingsbevoegdheden met enigszins minder relevantie	
126g Sv	Bevoegdheid voor de OvJ om te bevelen dat een opsporingsambtenaar stelselmatig een persoon volgt of diens aanwezigheid of gedrag waarneemt. Deze bevoegdheid is al van toepassing bij verdenking van een misdrijf.
126i Sv	Bevoegdheid voor de OvJ om te bevelen dat een opsporingsambtenaar een pseudo-koop of -dienstverlening uitvoert.
126ij Sv	Onder omstandigheden kan de bevoegdheid onder 126i Sv ook uitgevoerd worden door een burger.
126j Sv	Bevoegdheid voor de OvJ om een opsporingsambtenaar te bevelen dat hij zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar stelselmatig informatie inwint over de verdachte. Deze bevoegdheid is al toepasselijk bij verdenking van een misdrijf.
126h Sv	Bevoegdheid voor de OvJ om, onder bijkomende omstandigheden, te bevelen dat een opsporingsambtenaar deelneemt of medewerking verleent aan een groep van personen waarbinnen redelijkerwijs kan worden vermoed dat misdrijven worden beraamd of gepleegd.
126w Sv	Onder omstandigheden kan de bevoegdheid van 126h Sv uitgevoerd worden door een burger.

Bijlage 2 – Opsporingsbevoegdheden onder het nieuwe Wetboek van Strafvordering[86]

Onderzoeksbevoegdheid	Omschrijving
Inbeslagneming voorwerpen	
Artikel 2.7.7 NSv	Bevoegdheid voor de opsporingsambtenaar die een verdachte staande houdt of aanhoudt om voorwerpen die de verdachte met zich voert in beslag te nemen.
Artikel 2.7.8 NSv	Bevoegdheid van opsporingsambtenaar om voorwerpen in beslag genomen buiten artikel 2.2.7. NSv.
Artikel 2.7.9 NSv	Bevoegdheid voor opsporingsambtenaar om te bevelen dat iemand waarvan redelijkerwijs kan worden vermoed dat hij houder is van een voor beslagneming vatbaar voorwerp dit voorwerp uitlevert.
Artikel 2.7.10 NSv	Bevoegdheid voor opsporingsambtenaar om ter inbeslagneming elke plaats die niet een kantoor van een functioneel verschoningsgerechtigde is betreden en zoekend rondkijken.
Artikel 2.7.11 NSv	Bevoegdheid van de opsporingsambtenaar om ter inbeslagneming een vervoermiddel, met uitzondering van het woongedeelte zonder toestemming van de bewoner, te doorzoeken en zich toegang tot het vervoermiddel te verschaffen.
Artikel 2.7.12 NSv	Bevoegdheid voor de OvJ te bevelen dat een opsporingsambtenaar een plaats, met uitzondering van een woning zonder toestemming van de bewoner en een kantoor van een functioneel verschoningsgerechtigde, ter inbeslagneming doorzoekt.
Artikel 2.7.13 NSv	Bevoegdheid voor de OvJ om in gevallen waarin niet op het optreden van de R-C kan worden gewacht, te bevelen dat een opsporingsambtenaar een woning zonder toestemming van de bewoner of rechthebbende ter inbeslagneming doorzoekt.
Artikel 2.7.69 NSv	Bevoegdheid voor de R-C om op vordering van de OvJ of ambtshalve te bevelen dat een opsporingsambtenaar een woning zonder toestemming van de bewoner of een kantoor van een functioneel verschoningsgerechtigde doorzoekt ter inbeslagneming of voor het verrichten van onderzoek van gegevens.
Onderzoek van gegevens	
Artikel 2.7.37 NSv	Bevoegdheid voor de OvJ en opsporingsambtenaar om onder dezelfde voorwaarden als in artikel 2.7.10, 2.7.11, 2.7.12 en 2.7.13 NSv een plaats, vervoermiddel of woning te betreden of te doorzoeken.
Artikel 2.7.38 NSv	Bevoegdheid voor de R-C of de OvJ om te machtigen of bevelen dat er stelselmatig onderzoek van gegevens in een gegevensdrager of geautomatiseerd werk verricht wordt.

[86] Met betrekking tot de onderstaande tabel verdient opmerking dat het onderzoek aan het lichaam buiten beschouwing is gelaten vanwege het naar verwachting verminderde belang in zaken van online fraude.

Artikel 2.7.40 NSv	Bevoegdheid van de R-C of de OvJ te bevelen dat een opsporingsambtenaar een onderzoek van gegevens op een elders aanwezige gegevensdrager of geautomatiseerd werk wordt verricht.
Artikel 2.7.43 NSv	Bevoegdheid voor de OvJ om degene van wie redelijkerwijs vermoed kan worden dat hij beveiliging of versleuteling van een gegevensdrager of geautomatiseerd werk ongedaan kan maken, bevelen mede te werken aan het verkrijgen van toegang daartoe.
Verstrekking van gegevens	
Art 2.7.45 NSv	Bevoegdheid van de OvJ om degene die gegevens anders dan ten behoeve van persoonlijk gebruik verwerkt, waarvan redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen en gegevens waarvan redelijkerwijs kan worden aangenomen dat zij vatbaar zijn voor verlies of wijziging, bevelen dat deze gegevens worden bewaard en beschikbaar gesteld.
Artikel 2.7.46 NSv	Bevoegdheid voor de OvJ om degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde gegevens, te bevelen deze gegevens te verstrekken.