4 Verschijningsvormen van gedigitaliseerde criminaliteit

Jan-Jaap Oerlemans, Anne de Hingh & Wytske van der Wagen*

4.1 Inleiding

In dit hoofdstuk richten we ons op gedigitaliseerde criminaliteit. Gedigitaliseerde criminaliteit verwijst naar criminaliteit waarbij computers en internet als instrument worden gebruikt om traditionele criminaliteit te plegen (Tollenaar et al., 2019; Wall, 2014; zie ook hoofdstuk 1). In dit hoofdstuk gaan we dieper in op de meest voorkomende verschijningsvormen van gedigitaliseerde criminaliteit, te weten: strafbare feiten via online handelsplaatsen, witwassen en virtuele valuta, internetoplichting, online zedendelicten en online uitingsdelicten.

Voor een goed begrip van gedigitaliseerde criminaliteit leggen we eerst het verschil uit tussen het publieke internet (*clear web*), het *deep web* en het *dark web*. In de daaropvolgende paragrafen komen de verschillende verschijningsvormen van cybercriminaliteit en hun strafbaarstelling aan bod. Ten slotte richten we ons op de toekomst en presenteren we de studievragen en kernbegrippen met betrekking tot gedigitaliseerde criminaliteit.

4.2 De verschillende lagen van het internet: het clear, deep en dark web

Binnen de infrastructuur van het internet onderscheiden we drie lagen. Het publieke internet – ook wel clear web of *surface web* genoemd – is het direct toegankelijke deel van het internet, zoals de geïndexeerde websites die via de zoekmachine van Google met een standaard webbrowser te vinden zijn. Het

* Prof. mr. dr. J.J. Oerlemans is werkzaam als universitair docent Strafrecht bij het Instituut voor Strafrecht & Criminologie van de Universiteit Leiden. Daarnaast is hij bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht. Mr. dr. A.E. de Hingh is werkzaam als universitair docent bij de sectie Internetrecht van de Vrije Universiteit Amsterdam. Dr. W. van der Wagen is als criminoloog gespecialiseerd in cybercriminaliteit.

deep web is dat deel van het internet dat niet direct toegankelijk is en niet wordt geïndexeerd door zoekmachines, en waarvoor bijvoorbeeld eerst moet worden ingelogd of dat via een specifieke link toegankelijk is. Websites op het deep web zijn niet geïndexeerd door zoekmachines zoals Google of Bing. Hier kan worden gedacht aan webmail, privéprofielen op socialemediadiensten, of een wetenschappelijk artikel achter een betalingsmuur van een uitgever. Het dark web is dat deel van internet dat alleen bereikbaar is via een bepaald protocol en waar de IP-adressen van verbonden computers verborgen zijn.[1] Deze driedeling van het internet wordt vaak in de vorm van een ijsberg gepresenteerd:

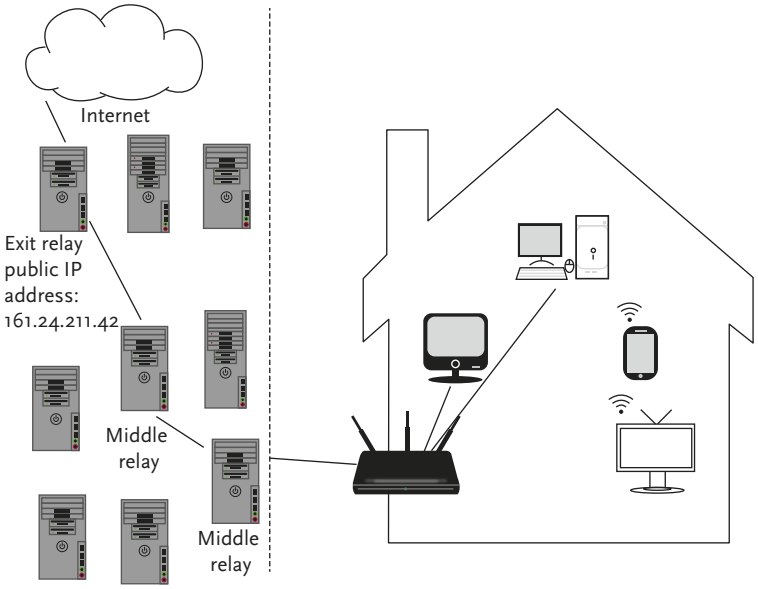
Figuur 4.1 Visualisatie van het onderscheid tussen het clear web, deep web en dark web[2]

Een *darknet* is een netwerk van computers die via een bepaald protocol communiceren en waarvan de IP-adressen verborgen zijn. Het is via een darknet mogelijk websites op het dark web te bezoeken. Een darknet is met andere woorden de infrastructuur die het bestaan van het dark web mogelijk maakt. Het bekendste systeem om verbinding te maken met een darknet is het systeem 'The Onion Router' (Tor). Tor kan als webbrowser door iedereen

1 Zie bijvoorbeeld A. Greenberg, 'Hacker Lexicon: What Is the Dark Web?', *Wired.com*, 19 november 2014.

2 Bron: Ranjithsiji, 'Iceberg of Webs', *Wikipedia.org*, 17 april 2018.

worden gedownload en geïnstalleerd. De werking van Tor is voor het eerst in een paper van Dingledine et al. (2004) uitgelegd. Het Tor-systeem stuurt internetverkeer langs (ten minste drie) servers en versleutelt ondertussen het netwerkverkeer. De tussenliggende Tor-servers leggen geen gegevens vast en alleen het IP-adres van de laatste Tor-server (ook wel *Tor exit node* of *Tor exit relay* genoemd) is zichtbaar. In figuur 4.2 is een internetverbinding via het Tor-systeem vanuit een woning met breedbandinternet gevisualiseerd.



Figuur 4.2 Visualisatie van een Tor-verbinding vanuit een woning[3]

Naast de voordelen van (meer) anonimiteit door het verhullen van het originele IP-adres van de computers die via het systeem verbinding maken en door versleuteld internetverkeer, maakt het Tor-systeem het ook mogelijk bepaalde diensten te benaderen die niet op het clear web en deep web staan. De diensten die alleen via een darknet, zoals Tor, toegankelijk zijn worden *hidden services* genoemd.[4] Daarbij kan worden gedacht aan websites, forums, chatdiensten en e-maildiensten.

3 Bron: Oerlemans, 2017a, p. 41.

4 Naast Tor zijn er ook andere programma's waarmee toegang kan worden verkregen tot darknets, zoals I2P en Freenet.

De anonimiteit die het Tor-systeem internetgebruikers biedt, maakt het aantrekkelijk voor criminelen. Tegelijkertijd wordt Tor ook gebruikt voor internetgebruikers die simpelweg meer privacy willen hebben en anoniemer van het internet gebruik willen maken. Daarbij moet ook worden gedacht aan journalisten die hun bronnen willen beschermen en relatief veilig willen communiceren of mensen die leven in dictatoriale regimes en ook graag niet-gecensureerde nieuwsbronnen willen lezen of met gelijkgezinden willen communiceren (Gehl, 2018).

4.3 Online handelsplaatsen

Online handelsplaatsen zijn plaatsen (forums) op het internet waar vraag en aanbod samenkomen. Binnen de context van dit boek hebben we het dan over de (illegale) handel in goederen (zoals drugs en wapens), diensten (zoals hacking tools) of gegevens (van slachtoffers). Online handelsplaatsen zijn qua functie goed te vergelijken met een winkelcentrum in de fysieke wereld of webshops op internet (Copeland et al., 2020; Odabaş et al., 2017; Smirnova & Holt, 2017) en zijn, zoals we zullen uitleggen, zowel te vinden op het clear web als het dark web.

Internetforums werken met gespecialiseerde software die gesprekken in een bepaalde volgorde weergeven en zijn gestructureerd rondom onderwerpen op zogenoemde subforums. Binnen deze subforums kunnen individuen een *thread* starten door een bericht te plaatsen met een vraag of met de wens om een bepaald product te kopen of te verkopen. In de context van markten waar goederen of diensten worden verkocht, houden verkopers doorgaans hun eigen threads bij waarin ze producten waarmee ze adverteren kunnen updaten. Leveranciers posten hier gedetailleerde informatie over het betalingsproces, de communicatiemiddelen en de levering van de goederen. Ook kunnen ze uitleg geven over hoe in het geval van niet-functioneren van goederen of diensten terugbetalingen kunnen worden geregeld of producten geruild kunnen worden. Klanten kunnen vervolgens ook beoordelingen of feedback achterlaten over de kwaliteit van de geleverde goederen of diensten (Dupont et al., 2017; Holt, 2013a; 2013b; Holt & Lampke, 2010; Madarie et al., 2023).

Internetforums en online handelsplaatsen worden ook wel 'cybercrime ontmoetingsplaatsen' genoemd (*cybercriminal convergence settings*) (Soudijn & Zegers, 2012; Leukfeldt et al., 2017c; Roks & Monshouwer, 2020). Het is een stabiele en voorspelbare plek waar cybercriminelen samenkomen en biedt

structuur en continuïteit aan mensen (Felson, 2003). Fysieke voorbeelden zijn bijvoorbeeld cafés, parken en *safe houses*. Bij online ontmoetingsplaatsen worden drie functies onderscheiden: (1) de marktfunctie; (2) de sociale functie; (3) de leerfunctie. De marktfunctie betreft de handel in illegale goederen en gegevens, de sociale functie gaat over het gebruik van platforms om te verbinden en te interacteren met anderen potentiële daders en de leerfunctie gaat over het uitwisselen van informatie en kennis tussen de deelnemers (Leukfeldt et al., 2017).

Naast online handelsplaatsen bestaan er ook 'shops' met één leverancier (een *single vendor shop*). Hier kunnen individuen specifieke producten rechtstreeks aan klanten verkopen zonder de directe concurrentie die wel aanwezig is op forums en cryptomarkten (Décary-Hétu et al., 2016; Smirnova & Holt, 2017). Deze sites maken gebruik van gemeenschappelijke e-commercetools en -platforms om efficiënt in contact te komen met klanten en goederen te distribueren (Hutchings & Clayton, 2016; Martin, 2014; Smirnova & Holt, 2017). Bovendien kunnen leveranciers advertenties op forums en cryptomarkten koppelen aan hun eigen winkels om hun producten beter in de cybercriminele markt te zetten (Ablon et al., 2014; Martin, 2014; Smirnova & Holt, 2017). In dit hoofdstuk richten we ons verder alleen op online handelsplaatsen. In het nu volgende komen de volgende verschijningsvormen van online handelsplaatsen en strafbaarstellingen aan bod: handelsplaatsen op het clear web, handelsplaatsen op het dark web (*darknet markets*) en handelsplaatsen op communicatie-apps.

4.3.1 Handelsplaatsen op het clear web

We denken vaak dat alle illegale handel op het dark web plaatsvindt, maar dat is niet het geval. Ook websites of forums op het publieke internet kunnen als (malafide) webwinkel fungeren waarop illegale goederen, zoals drugs en wapens, illegale diensten (zoals witwasdiensten of toegang tot gehackte computers) of gestolen informatie (bijvoorbeeld creditcard- of persoonsgegevens) worden aangeboden.

Als het gaat om drugshandel op het clear web onderscheidt het Trimbos-instituut[5] bijvoorbeeld twee soorten webshops, namelijk (1) webshops die middelen aanbieden die op de opiumlijst staan (deze middelen zijn aangemerkt in de Opiumwet) en (2) webshops die psychoactieve middelen verkopen die vaak afgeleid zijn van reeds bestaande drugs en nog niet op de opiumlijst staan

5 Het Trimbos-instituut is de instantie die drugsgebruik in Nederland onderzoekt.

(zie ook Olijhoek et al., 2021). Sommige online webshops doen zich voor als online 'apotheek' waar drugs zoals cocaïne of XTC besteld kunnen worden (Van Beek et al., 2023).

Casus: Wolkenwietje

In 2008 zag een ondernemende Hagenaar een gat in de drugsmarkt: de online verkoop van (soft)drugs.[6] Waar je met een fysieke coffeeshop slechts klanten in de regio kunt bedienen, heb je via internet immers een wereldwijd bereik. Daarmee was 'Wolkenwietje.nl' geboren, vermoedelijk de eerste online webwinkel voor (soft)drugs die opereerde vanuit Nederland. Al snel werd de website op verzoek van de politie offline gehaald.

Tot dusver krijgen online coffeeshops in Nederland geen gedoogvergunning. Een van de redenen is dat online coffeeshops praktisch gezien niet goed kunnen voldoen aan alle gedoogcriteria, zoals het controleren van de leeftijd en nationaliteit van de kopers en het verbod op adverteren via internet.[7]

Casus: RaidForums

RaidForums is een ander voorbeeld van een website op het clear web waar illegaal materiaal werd verspreid.[8] Op dit internetforum werden tussen 2015 en 2022 gehackte en gekopieerde gegevens, hacking tools en pornografisch materiaal verspreid. Mensen konden zich eenvoudig aanmelden op het forum en op subpagina's zoals 'Leaks Market' en daarmee toegang krijgen tot het materiaal dat werd aangeboden op de online handelsplaats. Zo werden op RaidForums gegevens van 700

6 'Politie sluit digitale coffeeshop', *Telegraaf.nl*, 19 maart 2008.

7 Zie de Aanwijzing Opiumwet, *Stcrt.* 2015, 5391.

8 Het woord 'raid' in RaidForums is een knipoog naar het begin van het forum in 2015, toen het vooral een online plek was voor het organiseren en ondersteunen van verschillende vormen van online intimidatie, zoals het sturen van de politie naar een adres van een nietsvermoedend onschuldig persoon.

miljoen LinkedIn-gebruikers aangeboden.[9] In totaal werden meer dan 10 miljard bestanden aangeboden. Het forum had naar verluidt meer dan een half miljoen leden.[10]

Het forum werkte met een systeem van *credits* waarmee leden toegang kregen tot bevoorrechte delen van de website en gecompromitteerde databases konden 'ontgrendelen' en downloaden. Leden konden ook op andere manieren credits verdienen, zoals door instructies te posten over hoe bepaalde illegale handelingen te verrichten.[11]

De website werd door de FBI en andere politiediensten op 12 april 2022 ontoegankelijk gemaakt waarbij de webservers in beslag werden genomen. De autoriteiten konden mogelijk al langer meekijken met de transacties die plaatsvonden op het forum.[12] In 2023 zijn in Nederland drie verdachten aangehouden en bleek de website duizenden Nederlandse gebruikers te hebben. Het is beleid dat, afhankelijk van de activiteit op een dergelijk forum, de gebruikers van de politie een e-mail of een brief ontvangen met daarin de mededeling dat ze gebruikers zijn van een onlangs offline gehaald forum, de nadrukkelijke oproep te stoppen met de activiteiten en een waarschuwing betreffende de gevolgen die het kan hebben als men zich schuldig maakt aan online criminaliteit. Minderjarigen kregen een stopgesprek met de politie.[13]

4.3.2 Handelsplaatsen op het dark web

Veel criminele marktplaatsen bevinden zich op het dark web. Deze handelsplaatsen worden ook wel darknet markets of *cryptomarkets* genoemd. De naam 'darknet market' weerspiegelt het gebruik van een op Tor gebaseerde site die alleen toegankelijk is voor andere Tor-gebruikers, waarbij de naam cryptomarket uitdrukt dat betalingen worden gedaan via zogenoemde *crypto-*

9 L. Mathews, 'Details On 700 Million LinkedIn Users For Sale On Notorious Hacking Forum', *Forbes.com*, 29 juni 2021.

10 Europol, 'One of the world's biggest hacker forums taken down', Europol, 12 april 2022.

11 United States Attorney's Office, 'U.S. Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator', 12 april 2022.

12 S. Lyngaas, 'FBI and international partners seize control of popular hacking forum', *CNN.com*, 12 april 2022.

13 'Politie benadert afnemers gestolen data', *politie.nl*, 12 april 2023.

currencies zoals bitcoin of monero (Barratt, 2012; Martin, 2014, zie ook paragraaf 4.4). Nog een ander kenmerk van deze markten is dat de levering van het product per post plaatsvindt (Verburgh et al., 2018). Silk Road – een van de eerste bekende darknetmarkten (zie casus) – groeide uit tot een belangrijke bron voor de verkoop van drugs en genereerde dermate veel aandacht dat dit resulteerde in een onderzoek door de FBI en de arrestatie van de exploitant Ross Ulbricht – ook wel bekend onder zijn *username* 'Dread Pirate Roberts' – in oktober 2013. Deze online handelsplaatsen maakten tot 2022 een groei door met in 2021 een enorme piek in de verkoop van drugs, wapens en hacktools op het dark web (Décary-Hétu & Giommoni, 2017; UNODC, 2023).[14]

Op darknetmarken wordt een grote verscheidenheid aan illegale producten en diensten verhandeld. Van drugs en wapens tot cybercriminele tools en gestolen gegevens (zie o.a. Broadhurst et al., 2018; Broadhurst et al., 2021; Holt & Lampke, 2010; Holt & Lee, 2022; Martin, 2014; Ouellet et al., 2022; Soska & Christin, 2015; Van Wegberg et al., 2018). Met betrekking tot wapenhandel gaat het bijvoorbeeld om een veelzijdig aanbod van wapens, van eenvoudige pistolen tot geavanceerde militaire wapens (Holt & Lee, 2023), maar denk ook aan tasers, messen, explosieven en munitie (Broadhurst et al., 2021). Vermeldenswaardig is dat wapens op deze online handelsplaatsen vele malen duurder zijn dan via het open web of via officiële offline verkooppunten in de Verenigde Staten (Holt & Lee, 2023).

Hoe succesvol de marktplaatsen zijn en de winst die ze vergaren, verschilt echter wel enorm. Volgens de United Nations Office on Drugs and Crime (UNODC, 2023) was de omzet van darknetmarkten in 2016 van honderden miljoenen dollars gegroeid naar 2,1 miljard dollar in 2021. Voor de handel in gestolen gegevens gaat het volgens Howell et al. (2023), die dertig darknetmarkten analyseerden, naar schatting ook om vele miljoenen. Schattingen ten aanzien van de wapenhandel via het dark web liggen op 960.000 per jaar (Holt & Lee, 2023).

Op darknetmarkten en forums heerst vaak een strikte hiërarchie. Met verschillende taken en verantwoordelijkheden wordt getracht de orde te handhaven en onwenselijke leden of herrieschoppers te verwijderen. 'Administrators' bepalen de regels, het doel en de richting van het forum of de marktplaats. 'Moderators' houden vaak toezicht op het forum en wijzigen of passen de inhoud op de website aan. Dit zijn vaak personen die experts zijn op een

14 Sinds 2022 is de markt door politieoperaties kleiner geworden en is het volgens het UNODC lastiger deze markten te volgen en inschattingen te maken van de omzet.

bepaald gebied en worden vertrouwd door de administrator. Verkopers (*vendors*) kunnen, zoals eerder benoemd, vaak een bepaalde status krijgen door goede beoordelingen (*reviews*) van klanten. De kwaliteit van hun producten en het leveringsproces worden daarbij constant beoordeeld (Holt, 2012). Klanten baseren er hun beslissing op om van de aangeboden diensten gebruik te maken (Szgeti et al., 2023). Het belang van reviews komt bijvoorbeeld duidelijk naar voren in het volgende citaat van een wapenverkoper op het dark web (Holt & Lee, 2023, p. 523-524).

> 'It's really important to leave a review after purchase. Reviews can only be left by "verified owners". We sold already a lot of products [on this cryptomarket] but no one left a review of the purchased product, despite the fact that users are satisfied with the purchased products and are happy to come back for more. So please leave review and let know everyone else about your opinion. It is also important for me and other people who work hard on this shop to make our service better. We want to be sure that our products will have appropriate descriptions and an adequate price for the value of the file. Anyone who leaves reviews under the purchased product will receive a discount code for subsequent purchases entitling to a 40% discount.'

Het verdienmodel van darknetmarkten is doorgaans als volgt. Voor elke transactie tussen een koper en verkoper krijgt de beheerder van de 'webshop voor drugs'[15] een klein percentage in cryptocurrency. De darknetmarkt faciliteert ook vaak in de transactie door als derde partij de fondsen vast te houden tot de koper groen licht geeft en de betaling kan overgaan naar de verkoper (dit wordt *escrow* genoemd).

Casus: Silk Road

Silk Road' was van 2011 tot 2013 een van de grootste en modernste online drugshandelsplaatsen op het internet en werkte ook op de hierboven beschreven manier.[16] In het geval van Silk Road bleek de administrator na twee jaar werk bij zijn arrestatie 28 miljoen dollar te

15 Typering in klare taal door de rechtbank Rotterdam in haar uitspraak over een online drugsmarkt. Zie Rb. Rotterdam 16 juli 2019, ECLI:NL:RBROT:2019:5630.

16 Zie uitgebreid J. Bearman, 'The Rise and Fall of Silk Road', *Wired Magazine*, 23 mei 2015, en het interactieve achtergrondverhaal 'Marktplaats van de drugs. De opkomst en ondergang van de digitale drugsmarktplaats', *de Volkskrant* op www.volkskrant.nl/kijkverder/2015.

hebben opgeslagen in zijn digitale portemonnee. Het geld werd uiteindelijk via een veiling verkocht en Ross Ulbricht kreeg een levenslange gevangenisstraf opgelegd.[17] Het verhaal van Silk Road geeft een inkijkje in de schaal en de mate van professionaliteit van drugshandel via het dark web. Na Silk Road volgden ook vele andere online handelsplaatsen in drugs op het dark web. Veel van deze drugsmarktplaatsen zijn inmiddels door politieoperaties offline gehaald en sommige darknetmarkten stopten zelf en namen de vastgehouden fondsen in het escrow mee (een *exit scam*).[18] Voorbeelden daarvan zijn Silk Road 2.0 (2014), AlphaBay (2017) en Hansa (2017), DreamMarket (2019), Hydra (2022), Van Wegberg & Verburgh (2018), Maras et al. (2023) en Goonetilleke et al. (2023).

Het Trimbos-instituut wees overigens in 2017 ook op de keerzijde van het sluiten van online marktplaatsen. Het betoogde destijds dat het kopen van drugs via internet veiliger is voor de gebruikers dan op straat. Bovendien geven de beoordelings- en betaalsystemen die online marktplaatsen hanteren, consumenten meer waarborgen over de geboden waar en levering.[19]

4.3.3 Handelsplaatsen op communicatie-apps

Zoals reeds is uitgelegd, is het doorgaans nodig om Tor te gebruiken om verbinding te maken met een (verborgen) webserver van een online handelsplaats op het dark web (oftewel een darknetmarkt). Het feit dat hiervoor enige technische competentie nodig is, werpt drempels op bij de aankoop van bijvoorbeeld drugs, waardoor gebruikers sneller kiezen voor socialemediadiensten en communicatieapps (Barratt & Aldridge, 2016; Van Beek et al., 2023). Dit brengt ons bij de toenemende handel in goederen en diensten via

17 S. Thielman, 'Silk Road operator Ross Ulbricht sentenced to life in prison', *The Guardian*, 29 mei 2015. De 144.336 bitcoins waren destijds meer dan 28 miljoen dollar waard. Zie ook het persbericht 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', U.S. Department of Justice, 16 januari 2014.

18 Zie bijvoorbeeld: A. Greenberg, 'The Dark Web's Top Drug Market, Evolution, Just Vanished', *Wired.com*, 18 maart 2015.

19 M. Hijink & L. van Lonkuyzen, 'Platleggen drugshandel op internet werkt averechts', *NRC.nl*, 28 augustus 2017.

socialemediaplatforms en communicatieapps (Salinas, 2018; Demant et al., 2019; Moyle et al., 2019; Søgaard, 2019).

Sociale media worden gebruikt als manier om te communiceren tussen bekenden over de aanschaf van bijvoorbeeld verdovende middelen, maar ook als platformen waarop, afhankelijk van de technische functionaliteiten, commerciële dealers hun producten en diensten kunnen aanbieden om nieuwe potentiële klanten te bereiken (Moyle et al., 2019). In de beschikbare onderzoeken, die zich overwegend richten op digitale drugsmarkten, wordt vooral gewezen op de populariteit van Snapchat, Instagram en Facebook voor de handel in verdovende middelen (Demant et al., 2019; Moyle et al., 2019; Bakken & Demant, 2019; Bakken, 2020, UNODC, 2023). Er is echter steeds meer empirisch bewijs dat er op dergelijke plekken ook een levendige handel is in tools en diensten gerelateerd aan cybercriminaliteit en in het bijzonder allerlei vormen van fraude (zie o.a. Bekkers & Leukfeldt, 2022; Bekkers et al., 2023). Hoe grootschalig deze handel is en hoeveel winst wordt gemaakt is niet bekend.

Uit onderzoek blijkt dat communicatieapps zoals Whatsapp, maar vooral ook Telegram worden gebruikt voor de handel in illegale diensten, goederen en gegevens, voor online zedendelicten en online vormen van fraude en oplichting (Van Beek et al., 2023; Garkava et al., 2024; Roks & Monshouwer, 2020).[20] Telegram Messenger is een gratis berichtendienst die gebruikers de mogelijkheid biedt om versleutelde berichten, foto's en videobestanden te delen die bovendien een zelfvernietigingsfunctie toegewezen kunnen krijgen (Moyle et al., 2019). Op Telegram worden berichten en bestanden versleuteld opgeslagen en daarnaast hebben gebruikers de mogelijkheid door middel van end-to-end encryptie in de zogenoemde 'Secret Chats' nog anoniemer te communiceren. Deze functie wordt doorgaans gebruikt als kopers geïnteresseerd zijn (Garkava et al., 2024). Door deze functionaliteiten presenteert Telegram zich als een veilige berichtendienst die bovendien laagdrempeliger is in termen van toegang en gebruik dan bijvoorbeeld forums op het dark web (Roks & Monshouwer, 2020; Roks & Hendriksen, 2021).

Als mensen in een groepsapp of kanaal (zoals op Telegram) handel gaan drijven ontstaat er een online handelsplaats. De beheerders van kanalen vervullen daarbij een belangrijke rol. Zij bepalen wie toegang krijgt tot de groep, bepalen de regels en de sancties en monitoren daarop (Dewey & Buzetti, 2024).

20 I. de Zwaan, 'Telegram is het nieuwe darkweb voor kinderporno: "Zelfs onze rechercheurs werden stil van de beelden"', *Volkskrant.nl*, 5 april 2024.

Een belangrijk verschil tussen communicatieapps en online handelsplaatsen op het darkweb, is dat via communicatieapps direct contact kan worden gelegd en het goed (bijvoorbeeld drugs) snel kan worden afgeleverd (Childs et al., 2020). Daarnaast is het zoals eerder genoemd eenvoudiger drugs aan te kopen via een communicatieapp dan op het dark web, omdat voor dat laatste enige technische expertise is vereist (Moyle et al., 2019). Garkava et al. (2024) wijzen ook op overeenkomsten in typen online markten, zoals het bij voorkeur gebruiken van cryptocurrencies, regels over wat is toegestaan en verboden op de marktplaatsen, de beschikbaarheid van handleidingen en uitleg en het gebruik van escrow diensten voor de transacties (zie ook Hutching & Holt, 2015). Garkava et al. vermoeden dat het voor gebruikers van Telegram lastiger is in te schatten of een groep of kanaal op Telegram betrouwbaar is, vanwege de andere structuur (met een centralere rol voor de beheerder) en het gebrek aan een reviewsysteem.

Het Trimbos-instituut stelde in 2023 vast dat in Nederland door jongvolwassenen het vaakst WhatsApp wordt gebruikt om in contact te komen met iemand die drugs verkoopt. Het gebruik van socialemediaplatformen (zoals Facebook en Instagram) om drugs te kopen wordt daarentegen weinig gemeld. In de etnografische studie van Demant et al. (2009) daarentegen werd geconstateerd dat er wel veel handel plaatsvindt via Facebook, Instagram, Snapchat en Facebook. Op Telegram worden op publiektoegankelijke kanalen – met vaak duizenden leden – dan weer honderden bestellijsten voor drugs gedeeld, soms met foto's van aangeboden producten erbij. Een verschil met Whatsapp is dat het bij Telegram om grote handelshoeveelheden gaat en Telegram de mogelijkheid biedt via zoekwoorden en op regio te zoeken (Van Beek et al., 2023). Ten slotte wijst het Trimbos-instituut erop dat ook van combinaties van platforms gebruik wordt gemaakt bij het aankopen van drugs, zoals bijvoorbeeld het delen van links naar webshops op het clear net én het dark web (Van Beek et al., 2023).

4.3.4 Strafbaarstelling

Met betrekking tot de strafbaarstelling van illegale handel op online marktplaatsen is er weinig nieuws onder de zon. Handel in illegale goederen, zoals drugs en wapens, is in Nederland strafbaar gesteld via de Opiumwet, de Wet wapens en munitie en andere bijzondere strafwetgeving. Op deze wetgeving buiten het Wetboek van Strafrecht wordt hier verder niet ingegaan.

Met betrekking tot de illegale handel in malware, ddos-diensten en gelekte gegevens zijn specifieke strafbaarstellingen naar aanleiding van de Wet computercriminaliteit II van belang, zoals besproken in hoofdstuk 3. Het vervaardigen, het bezit en de verspreiding van kwaadaardige software met het oogmerk delicten zoals computervredebreuk of ddos-aanvallen te plegen, zijn bijvoorbeeld strafbaar gesteld in artikel 139d Sr. Ook het voorhanden hebben, verkopen en verspreiden van computerwachtwoorden, toegangscodes en inloggegevens – met het oogmerk de gespecifieerde computerdelicten te plegen – zijn in artikel 139d Sr strafbaar gesteld. Het voorhanden hebben van gegevens om oplichting en fraude te plegen (zoals phishingmails of phishingwebsites) is strafbaar gesteld in artikel 234 Sr.[21]

Ten slotte is met de Wet computercriminaliteit III het 'helen van gegevens' strafbaar gesteld in artikel 139g Sr. Het gaat daarbij bijvoorbeeld om het aanbieden van gelekte of 'gestolen' gegevens op een online handelsplaats. Ook het kopen of voorhanden hebben van op online handelsplaatsen aangekochte gegevens kan strafbaar zijn op grond van artikel 139g Sr.

Casus: veroordeling voor handel op RaidForums

Op 3 november 2023 heeft de rechtbank Amsterdam een Nederlandse hacker veroordeeld voor onder meer computervredebreuk, afpersing, heling van niet-openbare gegevens, ransomware en het witwassen van een bedrag van meer dan een miljoen euro.[22]

In deze zaak had de verdachte gestolen databases met gegevens van 7,3 miljoen personen in zijn bezit, die hij zelf door middel van een hack verkregen had. Het ging daarbij onder meer om gegevens van Nederlandse bedrijven, zoals Ticketcounter. Bij dat bedrijf ging het om persoonlijke gegevens van honderdduizenden Nederlanders die via Ticketcounter een toegangskaartje hadden gekocht voor een pretpark, dierentuin, evenement of museum. Gegevens van 1,5 miljoen ticketkopers, met daarin ook geboortedatums, adressen, telefoonnummers en bankrekeningnummers werden aangeboden op hackersforum

21 Zie ook Rb. Rotterdam 6 februari 2024, ECLI:NL:RBROT:2024:699 n.a.v. Operation Cookie Monster.

22 Zie Rb. Amsterdam 3 november 2023, ECLI:NL:RBAMS:2023:6967.

RaidForums.[23] Verder ging het bijvoorbeeld om de gegevens van een gezondheidsorganisatie en een internetforum voor prostitutieklanten die slachtoffer werden van afpersing.[24]

De verdachte kreeg een gevangenisstraf opgelegd van vier jaar, waarvan één jaar voorwaardelijk. Deze zaak laat wederom zien dat een zaak kan leiden tot veroordelingen met betrekking tot zowel cybercriminaliteit in enge zin als gedigitaliseerde criminaliteit.

4.4 Witwassen met virtuele valuta

Cryptocurrencies, zoals bitcoin en monero, worden ook gebruikt om illegale goederen en diensten te kopen en geld wit te wassen. Het betreft virtuele valuta die zijn gebaseerd op cryptografische software en waarbij er geen centrale autoriteit is die toeziet op het beheer van het geld (zie o.a. Oerlemans et al., 2016).

Door de overheid worden cryptovaluta dan ook niet gezien als officieel 'echt geld' (fiduciaire valuta, zoals euro's en dollars) en elektronisch geld (op een bankrekening). Virtuele valuta zijn slechts bits en bytes waaraan door personen waarde wordt toegekend.[25] De Nederlandse wetgever en instituties lijken daarin op korte termijn geen verandering aan te willen brengen. De Nederlandsche Bank (DNB) schreef bijvoorbeeld in haar 'Visie op betalen 2022-2025' dat de volatiliteit (hevige schommelingen in de koers) van cryptovaluta ze ongeschikt maakt als algemeen geaccepteerd betaalmiddel.

Bitcointransacties gaan als volgt in hun werk. Bij de bitcoin verifieert een netwerk van bitcoingebruikers tezamen of een transactie legitiem is of niet. Het netwerk fungeert als een soort register en dat register wordt ook wel de 'blockchain' genoemd. Bitcoins worden verstuurd naar een bitcoinadres,

23 S. Hulsen, 'Hoe Ticketcounter-directeur Sjoerd na datadiefstal appte met een crimineel', *RTL Nieuws*, 23 februari 2023.

24 Redactie Noord-Holland, 'OM eist zes jaar tegen Zandvoorter voor grootschalige datadiefstal: "Unieke zaak, qua aard en omvang"', *AD.nl*, 22 oktober 2023.

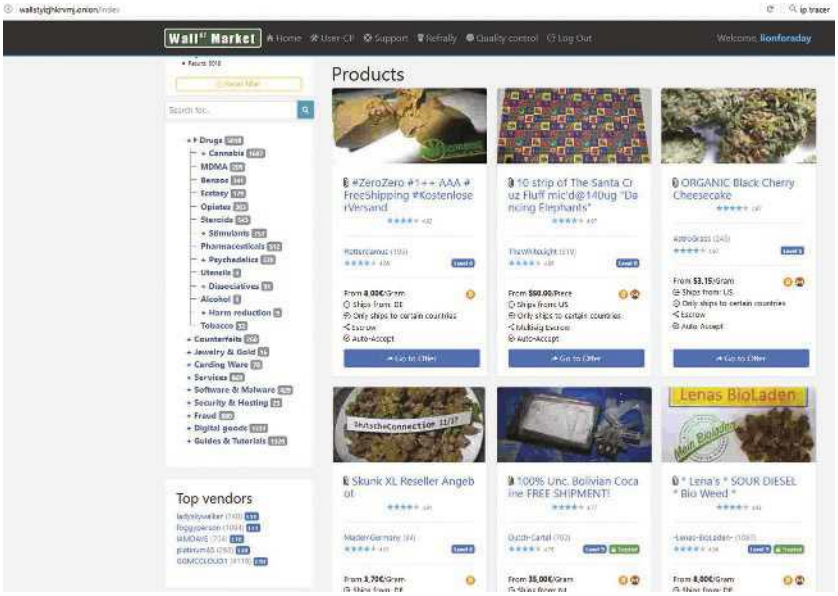
25 Virtuele valuta zijn in art. 1 Wet ter voorkoming van witwassen en financieren van terrorisme gedefinieerd als een 'digitale weergave van waarde', die als ruilmiddel wordt aanvaard, en 'elektronisch kan worden overgedragen, opgeslagen en verhandeld'.

zoals '1X6GYUigC9tYGqdNPJyL2769U9jd8P3vT', via een website of via apps die met de blockchain zijn verbonden. Alle transacties in de blockchain zijn openbaar en iedereen die dat wil, kan de transacties volgen. Bitcoins zijn dus niet anoniem, maar het is soms wel lastig de personen achter een bitcoinadres te identificeren. Als de identiteit van een gebruiker bekend raakt, bijvoorbeeld omdat de gebruiker die zelf prijsgeeft op het internet, kan diens hele transactiehistorie worden achterhaald. Bitcoins worden opgeslagen op een computer in een bestand, de zogeheten 'bitcoinwallet'. Deze digitale portemonnee is bereikbaar via een account van een internetgebruiker of bijvoorbeeld op een USB-stick. Via de digitale portemonnee is het ook mogelijk virtuele valuta over te dragen (over te maken) naar andere portemonnees.

Betalingen met cryptovaluta kunnen dus zonder tussenkomst van gereguleerde instellingen eenvoudig, snel en wereldwijd worden uitgevoerd. Een wallet en een cryptoadres zijn niet gekoppeld aan een naam van een natuurlijke persoon en geven hiermee een zekere mate van anonimiteit. Het gebrek aan toezichthouders en de relatieve anonimiteit zijn aantrekkelijk voor criminelen die bijvoorbeeld hun illegaal verkregen vermogen willen witwassen.[26] Het doel van witwassen is het versluieren van de herkomst van geld. Met andere woorden: illegaal geld een legale herkomst geven.[27] De relatie met cybercriminaliteit en virtuele valuta komt ook tot uiting bij het gebruik van ransomware, waarbij het losgeld bijna altijd in cryptocurrency moet worden overgemaakt (Custers, Oerlemans & Pool, 2020). Ook vinden betalingen op darknetmarkten voornamelijk in virtuele valuta plaats, zoals bitcoin en monero (Barratt, 2012; Martin, 2014).

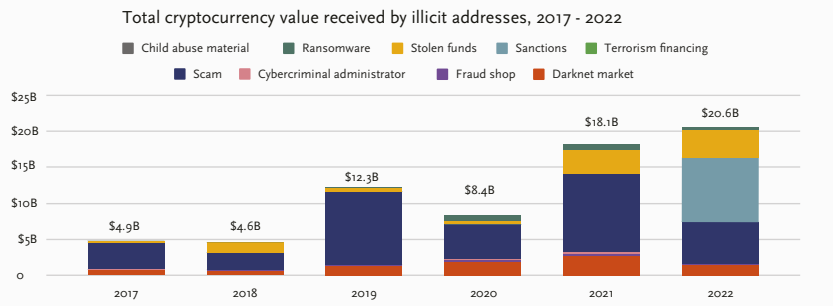
26 AMLC, 'Wat is witwassen met cryptovaluta?', 30 augustus 2023.

27 Zie ook Financial Intelligence Unit-Nederland, 'Wat is witwassen?', *fiu-nederland.nl*.



Figuur 4.3 Voorbeeld van een darknetmarkt met betalingsmogelijkheden in bitcoin en monero

Volgens het UNODC waren er in 2022 wereldwijd voor 20 miljard euro aan transacties die door het bedrijf ChainAlysis gelinkt zijn aan allerlei vormen van criminaliteit, namelijk: seksueel materiaal van minderjarigen, ransomware, gestolen (crypto)geld, geld dat naar landen ging die onder sancties vallen (zoals Rusland en Noord-Korea), geld dat is gebruikt voor de financiering van terrorisme, oplichting, administrators van cybercriminele groepen, nepwebwinkels en darknetmarkten (zie figuur 4.4).



Figuur 4.4 Geschatte waarde in miljarden dollars aan crimineel geld per sector[28]

4.4.1 Regulering

Met de implementatiewet van de vijfde Europese antiwitwasrichtlijn is een eerste stap gezet in de bestrijding van witwassen via cryptogeld.[29] Bepaalde cryptodienstverleners zijn nu gereguleerd in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Het gaat daarbij om (1) *crypto-omwisselplatforms*, waar men virtuele valuta kan omwisselen voor andere virtuele valuta (bijvoorbeeld van bitcoin naar monero of andersom) of virtuele valuta kan omwisselen naar fiat geld (bijvoorbeeld van bitcoin naar de euro of andersom); en (2) *cryptobewaarportemonnees* zoals de hiervoor genoemde 'bitcoinwallet'. Deze instanties zijn belangrijke aanknopingspunten voor opsporingsonderzoeken naar witwassen. Daders kunnen hun virtuele valuta immers niet altijd direct besteden bij reguliere winkels en moeten deze dan omzetten in fiduciair geld.

Als een aanbieder een van deze twee cryptodiensten beroeps- of bedrijfsmatig, in of vanuit Nederland aanbiedt, moet hij zich registreren bij DNB. De Wwft en de Sanctiewet bepalen dat deze bedrijven ook als 'poortwachters' moeten optreden. Daarom moeten zij maatregelen nemen om strafbare feiten, zoals witwassen en het financieren van terrorisme, tegen te gaan. De aanbieder is daarom verplicht om de identiteit van klanten verifiëren ('Know Your Customer' (KYC)-beleid) en moet monitoren op verdachte transacties. Ongebruikelijke transacties moeten worden gemeld bij de Financial Intelligence

28 Bron: 'UNODC calculations based on Chainalysis', in: *The 2023 Crypto Crime Report*, UNODC, februari 2023.

29 Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van richtlijn 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering.

Unit (FIU). De FIU-Nederland is een onderdeel van de Fiscale Inlichtingen- en Opsporingsdienst (FIOD).

DNB houdt toezicht op de naleving van deze bovengenoemde vereisten uit de Wwft.[30] Het niet naleven van de Wwft-vereisten is, naast bestuursrechtelijk, strafrechtelijk gesanctioneerd in de Wet op de economische delicten.

Verder is in 2023 Europese wetgeving aangenomen om witwassen met cryptovaluta tegen te gaan.[31] Deze regelgeving is breder dan de vijfde antiwitwasrichtlijn en ziet ook op andere cryptodiensten. De verordening stelt regels ten aanzien van onder andere consumentenbescherming, het tegengaan van marktmisbruik en andere eisen ten aanzien van de bedrijfsvoering van aanbieders van cryptodiensten. In Nederland wordt deze Europese regelgeving geïmplementeerd in het wetsvoorstel Uitvoeringswet verordening markten in cryptoactiva (zie verder ook o.a. Middelburg & Voerman, 2023).

Dit boek richt zich verder op de strafbaarstellingen in het Wetboek van Strafrecht en niet op deze andere wetgeving.

4.4.2 Strafbaarstelling

De strafbaarstelling van witwassen met virtuele valuta zoals bitcoin is hetzelfde als het witwassen met fiduciair (echt) geld. In artikel 420bis.1 Sr (eenvoudig witwassen) wordt enkel het verwerven of voorhanden hebben van een voorwerp dat onmiddellijk afkomstig is uit enig eigen misdrijf strafbaar gesteld, met een maximale gevangenisstraf van zes maanden. Daarbij kan het bijvoorbeeld gaan om bitcoins die zijn verkregen uit drugshandel op een darknetmarkt. Dit delict kan ten laste worden gelegd ter aanvulling van het gronddelict (het gepleegde misdrijf waarmee het geld wordt verdiend) én als delict ter vervanging van een (mogelijk) gronddelict.[32]

Ook het delict opzetwitwassen (art. 420bis Sr) komt veel voor bij virtuele valuta. Bij opzetwitwassen worden de versluierhandelingen (het verbergen of

30 De Autoriteit Financiële Markten (AFM) zal de vergunningen uitgeven voor cryptodienstaanbieders in het kader van de uitvoeringswet.

31 Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactivamarkten en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937.

32 Zie verder ook R.A. Regtering, 'Witwassen van virtuele valuta', *amlc.nl*, 31 oktober 2022.

verhullen van de oorsprong), de plaatsingshandelingen (verwerven, voorhanden hebben, overdragen of omzetten) en de omzettingshandelingen (omzetten en gebruikmaken) van een voorwerp[33] uit misdrijf verkregen, strafbaar gesteld. Op deze vorm van witwassen staat een maximumstraf van ten hoogste zes jaar of een geldboete van de vijfde categorie.[34] De strafbaarstellingen van witwassen worden niet alleen ingezet tegen (rechts)personen die direct betrokken zijn bij criminele activiteiten. Ook dienstverleners die hiertoe gelegenheid verschaffen kunnen worden vervolgd voor witwassen.

In de praktijk worden 'witwastypologieën' onderscheiden die van nut kunnen zijn voor de bewijsvoering voor witwassen met cryptovaluta (zie ook Oerlemans et al., 2016; Custers et al., 2020). De volgende indicatoren[35] voor transacties met cryptovaluta worden door het Anti Money Laundering Centre (AMLC) genoemd:

1. Het meermalen binnen een relatief korte periode vanaf bankrekening(en) opnemen van aanzienlijke contante bedragen, zonder een kennelijke economische noodzaak en in combinatie met het meermalen giraal ontvangen van bedragen. Hierbij kan sprake zijn van *cashing*, waarbij via pintransacties het geld wordt opgenomen en witgewassen.
2. De aankoop van virtuele betaalmiddelen waarbij, bijvoorbeeld, aan ten minste twee van de volgende situaties wordt voldaan:
   - de koper stelt geen identiteit van de verkoper vast;
   - de koper schermt de eigen identiteit af;
   - de koper rekent in contanten af;
   - de koper brengt een ongewoon hoog percentage wisselcommissie in rekening;
   - de transactie vindt plaats in een (openbare) omgeving waar veel publiek aanwezig is waardoor het veiligheidsrisico voor de koper vermindert;
3. De koper en/of verkoper maakt/maken bij de verkoop van virtuele betaalmiddelen gebruik van een zogenoemde bitcoinmixer. Een bitcoinmixer

33 Cryptocurrencies worden doorgaans als 'voorwerp' aangemerkt. Zie ook concl. A-G Aben 27 februari 2024, ECLI:NL:PHR:2024:216, r.o. 20-33.

34 Bij schuldwitwassen (art. 420quater Sr, maximaal twee jaren gevangenisstraf) gaat het om de versluierhandelingen en verplaatsingshandelingen van een voorwerp, waarbij de verdachte redelijkerwijs moet vermoeden dat het voorwerp uit een misdrijf afkomstig is. Bij gewoontewitwassen (art. 420ter Sr) worden zwaardere strafmaxima van acht jaren gesteld voor degene die een gewoonte maakt van het plegen van witwassen.

35 Deze lijst is door de auteurs ingekort en aangepast. Zie ook Hof Den Haag 1 februari 2022, ECLI:NL:GHDHA:2022:104, *Computerrecht* 2022/95, m.nt. J.J. Oerlemans & K.M.T. Helwegen (*zaak IJsberg*).

is een dienst waarbij tegen betaling van een commissie bitcoins tegen andere bitcoins worden gewisseld. De bitcoinmixer zorgt ervoor dat het volgen van transacties via de blockchain wordt verhinderd (Van Wegberg, Oerlemans & Van Deventer, 2018, Miedema et al., 2023). Door de mixer te gebruiken is de transactiegeschiedenis (in aard, omvang, wallets en partijen) niet te zien of te reconstrueren.

4. Accepteren, handelen in of beschikbaar hebben van *coins* met een historie op het dark web. Software van het bedrijf Chainalysis kan worden gebruikt om aan te tonen dat cryptovaluta afkomstig zijn uit online drugsmarktplaatsen.
5. Gebruik van een betaalkaart (*prepaid* kaart) die gevoed wordt door cryptovaluta.
6. Grote kasstortingen en -opnames via speciale geldautomaten voor cryptovaluta.
7. Transacties in cryptovaluta voor de aankoop van luxegoederen, die niet passen bij het aangegeven inkomen/vermogen.

Casus: witwassen van bitcoins afkomstig van Agora en Evolution Market

Op 10 maart 2017 heeft de rechtbank Noord-Nederland een verdachte veroordeeld voor online drugshandel en gewoontewitwassen.[36] De verdachte dreef een omvangrijke handel voornamelijk in xtc-pillen en LSD via de – indertijd populaire – darknetmarkten Agora en Evolution. De verdachte specialiseerde zich in het bevoorraden van de zogenoemde *resellers* en behoorde daarmee tot het hogere segment van de drugshandel. Voor de bewijsvoering is onder andere gebruikgemaakt van de beoordelingen van de drugshandelaar door klanten op de forums.

In de zaak wordt uitgebreid ingegaan op de gebruikte cryptocurrencies, in dit geval bitcoins, *paycoins* en *opalcoins*. Met behulp van financieel rechercheren zijn de rechercheurs nagegaan of er een verbinding gemaakt kon worden tussen de bitcoinadressen in de digitale portemonnee op de laptop van de verdachte en de transacties en bitcoinadressen die voorkomen op genoemde darknetmarkten. In de periode van 24 februari tot en met 9 maart 2015 waren bijvoorbeeld 889,90 bitcoins naar de forums overgemaakt met een toenmalige waarde van

36 Rb. Noord-Nederland 10 maart 2017, ECLI:NL:RBNHO:2017:1940.

208.125,72 euro. Daarbij is van zestien transacties vastgesteld dat de verdachte deze heeft ontvangen via Evolution Market of via Agora.

De verdachte is veroordeeld voor gewoontewitwassen. De herkomst van de cryptocurrencies (uit de online drugshandel) werd verhuld door het omwisselen van de bitcoins in euro's. Deze geldbedragen zijn afkomstig uit enig misdrijf. De rechtbank kwalificeert de aanschaf van de personenauto's en luxegoederen als verhullingshandelingen, nu deze zijn aangeschaft met geld afkomstig uit de handel in verdovende middelen. Het virtuele geld dat de verdachte nog in zijn bezit had en de luxegoederen worden door de rechtbank verbeurd verklaard. Ondanks de relatief jeugdige leeftijd van de verdachte tijdens het begaan van die feiten, wordt hij veroordeeld tot een gevangenisstraf van drie jaar.

4.5 Internetoplichting

Internetoplichting is een veelvoorkomende vorm van gedigitaliseerde criminaliteit. Het CBS rapporteert in de Veiligheidsmonitor (2024) dat mensen in 2023 het vaakst slachtoffer werden van online oplichting en fraude (9%), waarbij aankoopfraude het vaakst voorkwam (8%).

Voor internetoplichting wordt vaak de term *phishing* gebruikt: het hengelen (of 'vissen') naar persoonlijke en/of vertrouwelijke gegevens zoals gebruikersnamen, wachtwoorden, IP-adressen en bankgegevens. Phishing kan worden omschreven als een vorm van oplichting waarbij gegevens van een persoon worden verzameld door het doelwit te verleiden tot het verstrekken van persoonlijke of financiële informatie. Vaak gebeurt dit met behulp van een e-mail of bericht waarin een link is opgenomen naar een valse website (o.a. Loggen & Leukfeldt, 2022; Van der Wagen & Bernaards, 2020). Vervolgens wordt deze informatie verkocht aan derden of gebruikt door met die gegevens via internet bestellingen te plaatsen. Phishing gebeurt over het algemeen ongericht, waarbij hetzelfde phishingbericht in één keer naar een grote groep slachtoffers wordt gestuurd. Bij *spearphishing* daarentegen worden de overtuigingstechnieken specifiek aan het slachtoffer aangepast.

Doelwitten worden vaak verleid tot het delen van persoonlijke of financiële informatie via een website. Het opzetten van een phishingwebsite is eenvou-

dig geworden door de ontwikkeling van *phishingkits*. Deze software fungeert als hulpmiddel om deze websites op te zetten en kunnen gekocht, gehuurd, of zelfs gratis worden gedownload op darknetmarkten, socialemediaplatforms of communicatieapps, zoals Telegram. Vaak betreft de frauduleuze website een neponlinebankieromgeving of neponlinebetalingsplatform. De *gephiste* gegevens worden vaak verstuurd naar een e-mailadres of bij elkaar gebracht in een *phishingpanel* (Bijmans et al., 2021).[37] De aanvallen op doelwitten zijn vaak afgestemd op een bepaald publiek en land. Hoewel vaak de verwachting is dat phishingaanvallen technisch steeds geavanceerder worden, is de modus operandi volgens Loggen & Leukfeldt (2022) door de jaren heen nauwelijks veranderd.

Casus: betaalverzoekfraude

In deze casus nemen we als voorbeeld betaalverzoekfraude via Marktplaats.nl, een bekend Nederlands online handelsplatform (zie Rooyakkers & Weulen Kranenbarg, 2020, p. 30-33). Bij deze vorm van criminaliteit wordt een verkoper door een zogenaamd geïnteresseerde koper (hierna: fraudeur) met behulp van een gehackt Marktplaatsaccount benaderd via de Marktplaats-chat en/of via WhatsApp. Voor de fraudeur is het aantrekkelijk om te kiezen voor communicatie via WhatsApp, omdat detectie- en waarschuwsystemen van Marktplaats.nl daar niet werken.

Na contact vindt er een korte onderhandeling plaats, waarna er overeenstemming wordt bereikt over de verkoop (hierbij wordt vaak direct de vraagprijs geboden door de fraudeur). Nu er een deal is, stuurt de fraudeur een niet-legitiem betaalverzoeklinkje om 1 cent over te maken, zogenaamd om de identiteit van de verkoper te controleren en overtuigt deze het slachtoffer daarop te klikken. Als deze link verstuurd wordt binnen de omgeving van de Marktplaatschat gaat dit door middel van een *gatewaylink*, ofwel een *forwarder* naar een phishingsite. Als het contact is verlopen via WhatsApp klikt het slachtoffer op een URL (linkje) die lijkt op een legitiem betaalverzoek, inclusief bijbehorende logo's en tekstuele stijl. Door te klikken op de door de fraudeur verstuurde niet-legitieme betaalverzoeklink om het bedrag over te maken,

37 Zie ook Rb. Den Haag 1 juli 2021, ECLI:NL:RBDHA:2021:6678 over phishingpanels.

komt het slachtoffer op een phishingwebsite. Deze phishingsite heeft de *look and feel* van een legitiem betaalverzoek.

Op deze internetbankierenphishingsite worden vervolgens gegevens gevraagd zoals een gebruikersnaam, wachtwoord en betaalpasgegevens, om zogenaamd in te kunnen loggen op de internetbankierenomgeving ter afronding van de betaling. Op deze wijze en in de daaropvolgende handelingen worden door de fraudeur eveneens authenticatie- en verificatiecodes afgevangen. Met deze afgevangen gegevens logt de fraudeur in op het internetbankierenaccount van het slachtoffer en worden bijvoorbeeld telefoons of tablets die in het bezit zijn van de fraudeur gekoppeld aan de bankrekening van het slachtoffer. Zonder medeweten van het slachtoffer heeft de fraudeur nu toegang tot de bankrekening en kunnen transacties worden doorgevoerd.

De laatste stap is vervolgens het wegsluizen van het geld dat op de rekeningen staat waartoe de fraudeur nu toegang heeft (de *cash-out*). Alle onderdelen van deze modus operandi (zoals gehackte Marktplaatsaccounts en het phishingpanel) en bijbehorende kennis kunnen voor een lage prijs worden gekocht of ingehuurd via internet (Van Wegberg et al., 2018). Cash-out gebeurt vaak door middel van overboekingen naar geldezels, het plaatsen van online bestellingen (tegoedkaarten, cryptocurrency of bestellingen bij webshops) of betalingen in fysieke winkels (vanaf de telefoon, via de Apple Pay-betaalmethode). Vervolgens zal de fraudeur (indien er via WhatsApp contact is geweest) vaak de berichten wissen, zodat het slachtoffer bijvoorbeeld het telefoonnummer of de verstuurde phishing-URL niet meer kan opzoeken.

Slachtoffers worden ook vaak benaderd via Whatsapp of andere communicatieapps door daders met andere trucs, zoals bijvoorbeeld bij vriend-in-noodfraude. Daarbij doen daders zich voor als de dochter of zoon van het slachtoffer met de mededeling dat ze een nieuw nummer hebben. Al snel vragen ze vervolgens om geld, bijvoorbeeld omdat hun fiets of auto kapot is gegaan en zij geen beschikking hebben over een pinpas. Verder kan gedacht worden aan CEO-fraude als voorbeeld van (spear)phishing. Daarbij wordt de identiteit van de algemeen directeur (de Chief Executive Officer) (CEO) van een bedrijf misbruikt om – meestal via e-mail – bijvoorbeeld aan een medewerker van de financiële afdeling de opdracht te geven om een betaling uit te voeren

(Europol, 2016; 2018). Het bericht is zo veel mogelijk op maat gemaakt om het slachtoffer ervan te overtuigen geld over te maken. In Nederland zijn bijvoorbeeld twee bestuurders van Pathébioscopen voor 19 miljoen euro opgelicht via een phishing-e-mail.[38]

4.5.1 Strafbaarstelling

Internetoplichting is strafbaar gesteld als het delict oplichting in artikel 326 Sr. Daarvan is sprake als iemand door middel van een valse naam of hoedanigheid of 'listige kunstgrepen' goederen of gegevens van een ander afhandig maakt. Op het delict staat een maximale gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie. Als de daders zich voordoen als een andere persoon, kan er ook sprake zijn van identiteitsfraude in de zin van artikel 231b Sr.[39] Het maken en gebruikmaken van phishingmails kan ook strafbaar zijn op grond van artikel 139d en 234 Sr. Het betreft dan het voorhanden hebben van inloggegevens met de bedoeling om zich daarmee toegang te verschaffen tot het betalingsverkeer van anderen.[40] Als er gebruik wordt gemaakt van malware om ingevulde persoonsgegevens op websites afhandig te maken (bijvoorbeeld door middel van een *keylogger*), dan kan er uiteraard sprake zijn van een computerdelict zoals besproken in hoofdstuk 3. Als geld van de rekening van het slachtoffer wordt gepind of wordt overgemaakt door de dader naar een andere rekening is ook sprake van diefstal (art. 310 Sr), met behulp van de verworven toegangsgegevens en/of bankpas met bijbehorende pincode.[41] Wordt gebruikgemaakt van geldezels of andere verhullingshandelingen, dan kan er ook sprake zijn van witwassen in de zin van artikel 420bis Sr.

In de tenlastelegging bij phishingzaken wordt ook opvallend vaak 'deelname aan een criminele organisatie' als delict opgevoerd (art. 140 Sr). Gezien de veelvoorkomende rolverdeling is dat goed denkbaar. Daarbij moet wel sprake zijn van een duurzaam en gestructureerd samenwerkingsverband, waarbij wordt beoogd de in de tenlastelegging genoemde misdrijven te plegen.[42]

38 In een uitspraak van de sector civielrecht van de rechtbank Amsterdam over het ontslag van een van de bestuurders zijn veel details over de verstuurde e-mails te lezen: Rb. Amsterdam 31 oktober 2018, ECLI:NL:RBAMS:2018:7881.

39 Zie bijvoorbeeld Rb. Den Haag 6 maart 2020, ECLI:NL:RBDHA:2020:2595.

40 Zie bijvoorbeeld Hof Arnhem-Leeuwarden 15 december 2022, ECLI:NL:GHARL:2022:10845.

41 Zie bijvoorbeeld Hof Arnhem-Leeuwarden 15 december 2022, ECLI:NL:GHARL:2022:10845.

42 Zie bijvoorbeeld Rb. Amsterdam 9 november 2015, ECLI:NL:RBAMS:2015:8035.

Uiteraard moet het Openbaar Ministerie ook daarvoor het benodigde bewijs aandragen.

In de Wet computercriminaliteit III is ten slotte in artikel 326e Sr een nieuwe bepaling toegevoegd, waarin specifiek 'online handelsfraude' strafbaar wordt gesteld (Buisman, 2020). In deze nieuwe strafbaarstelling is vereist dat een 'beroep of gewoonte' wordt gemaakt van het niet (volledig) leveren van een product of dienst, maar dat men zich ondertussen wel verzekert van betaling. In de praktijk zullen in de eerste plaats private partijen deze vorm van fraude bestrijden. Als het echt noodzakelijk is, zullen de politie en het Openbaar Ministerie optreden, waarbij gebruik wordt gemaakt van gebundelde aangiften.[43]

Het eenvoudigweg niet leveren van een beloofd goed of beloofde dienst, bijvoorbeeld aangeboden op Marktplaats.nl, is geen oplichting, want daarvoor is in juridische zin het volgende vereist: 'het aannemen van een valse naam of hoedanigheid, listige kunstgrepen of een samenweefsel van verdichtsels'.[44] Als een beloofde dienst of beloofd goed niet wordt geleverd, dan moeten burgers in principe het burgerlijk recht toepassen en via die weg nakoming en dergelijke vorderen.

Op de website van de politie staat dat alle aangiftes van internetoplichting worden bekeken op aanknopingspunten voor verder onderzoek. Zo wordt bijvoorbeeld bekeken of een bankrekeningnummer, IP-adres, of e-mailadres naar een verdachte wijst of dat er misschien sprake is van meerdere aangiftes die met elkaar te maken hebben. Zo'n cluster van aangiftes kan wijzen op grootschalige oplichting. Met het Openbaar Ministerie wordt besproken welke zaken in aanmerking komen voor verder onderzoek. Er komen alleen zoveel meldingen binnen dat niet in alle gevallen een opsporingsonderzoek kan worden gestart.[45]

4.6 Online zedendelicten

De opkomst van het internet en de groeiende digitalisering hebben geleid tot nieuwe (online) zedendelicten en zijn ook van invloed geweest op bestaande zedenmisdrijven. Zo is het door het internet bijvoorbeeld veel eenvoudiger

43 Zie *Kamerstukken II* 2015/16, 34372, nr. 3, p. 75.
44 Zie ook het overzichtsarrest van HR 20 december 2016, ECLI:NL:HR:2016:2889.
45 'Internetoplichting en opsporingsonderzoek', *Poltie.nl*, 20 februari 2024.

geworden om seksueel beeldmateriaal, zoals materiaal van seksueel misbruik van kinderen, te verspreiden op een schaal die in de fysieke wereld vrijwel onmogelijk is (Taylor & Quayle, 2006). Het internet heeft ook het leggen van al dan niet anoniem contact over (grote) afstand mogelijk gemaakt waardoor misdrijven zoals 'virtuele aanranding' of aanranding op afstand (bijvoorbeeld door middel van afpersing) zijn opgekomen. In deze paragraaf worden enkele online zedendelicten behandeld waarbij het internet en ICT een essentiële rol spelen, of dienen als omgeving waarin of als medium waarop deze vormen van gedigitaliseerde criminaliteit plaatsvinden.

4.6.1 Beeldmateriaal van seksueel misbruik van minderjarigen

Bij het maken of verspreiden van materiaal van seksueel misbruik van kinderen spelen computers en internet nadrukkelijk en al jaren een belangrijke rol. De opkomst van het internet in de jaren negentig zorgde voor een mondiale verspreiding en groeiende online beschikbaarheid van materiaal van seksueel misbruik van kinderen. Dit komt bijvoorbeeld tot uiting in de zeer grote hoeveelheden materiaal die verdachten dikwijls in hun bezit blijken te hebben: in de jurisprudentie komen geregeld aantallen als honderdduizenden en zelfs miljoenen afbeeldingen van seksueel kindermisbruik voor (Van den Hurk et al., 2023).[46]

Hoewel de term 'kinderpornografie' lange tijd een ingeburgerde term was, wordt tegenwoordig de voorkeur gegeven aan de benaming '(beeld)materiaal van seksueel misbruik van minderjarigen' (Van der Bruggen, 2023).[47] Bij deze vorm van gedigitaliseerde criminaliteit is, eenvoudig gezegd, sprake van het maken of verspreiden van een foto of een video (maar ook van bijvoorbeeld een gif'je of een sticker, enz.) van een kind van jonger dan 18 jaar dat seksuele handelingen verricht, seksueel poseert of zich in een seksueel getinte omgeving bevindt.[48] In dit boek gebruiken wij zo veel mogelijk de term 'seksueel materiaal van minderjarigen'. De reden is dat deze term

46 Zie bijvoorbeeld Rb. Rotterdam 9 december 2009, ECLI:NL:RBROT:2009:BK6022, Rb. Den Haag 13 maart 2013, ECLI:NL:RBDHA:2013:2872, Rb. Rotterdam 31 maart 2017, ECLI:NL:RBROT:2017:2445 en Rb. Rotterdam 19 februari 2024, ECLI:NL:RBROT:2024:1928.

47 Zie ook Defense for Children, 'Terminologiegids seksueel misbruik en seksuele uitbuiting van kinderen', 2022. Overigens geeft de Nederlandse wetgever nog de voorkeur aan de term kinderpornografie omdat de alternatieve benamingen de reikwijdte van de Nederlandse strafbaarstelling van kinderpornografie niet volledig dekken, zie *Kamerstukken II* 2022/23, 36222, nr. 3, p. 26.

48 Zie 'Wat melden?', *Meldpunt-Kinderporno.nl*.

volgens ons het beste de strafbaarstelling van de gedraging in het wetsartikel reflecteert, waarbij niet altijd – letterlijk – sprake is van handelingen van seksueel misbruik.

De maatschappelijke opvattingen ten aanzien van seksueel materiaal van minderjarigen hebben door de jaren heen een duidelijke ontwikkeling doorgemaakt. De jaren zestig kenmerkten zich bijvoorbeeld als een tijd met een relatieve openheid en seksuele vrijheid en expressie, waarin seksueel contact tussen volwassenen en kinderen niet zonder meer werd afgewezen.[49] In die tijd kochten geïnteresseerden dergelijk materiaal in seksshops of via postorderbedrijven (Taylor & Quayle, 2003). Vanaf de jaren tachtig vond er een mentaliteitsverandering plaats. De toenmalige vrouwenbeweging benadrukte de schadelijke effecten van pornografisch materiaal en vanuit politie en justitie werd erop gewezen dat de productie van pornografisch materiaal waarop kinderen te zien zijn, vaak gepaard gaat met kindermisbruik (Kool, 1999). Eind jaren tachtig werd het maken en delen van afbeeldingen van seksueel misbruik van kinderen jonger dan 16 jaar dan ook strafbaar gesteld in artikel 240b Sr (oud), met destijds een maximale gevangenisstraf van drie maanden. In 1996 werd de strafmaat verhoogd naar vier jaar en in 2002 is de leeftijdsgrens van het slachtoffer in het toenmalige artikel 240b Sr verhoogd van 16 naar 18 jaar.

Ook vond er in de loop der jaren een verschuiving plaats van fysieke naar digitale ontmoetingsplekken of marktplaatsen van personen die interesse hebben in seksueel materiaal van minderjarigen. Van der Bruggen zet in haar werk uiteen hoe dit beeldmateriaal wordt uitgewisseld in professionele netwerken (forums) die via een darknet toegankelijk zijn (voornamelijk Tor). Op deze forums op het dark web zijn duizenden tot honderdduizenden personen bewust op zoek naar beeldmateriaal van seksueel misbruik van minderjarigen en bereid om de grens van het strafbare te overschrijden (Van der Bruggen, 2023). In tegenstelling tot andere online markten zoals drugs markets is daarbij geen sprake van een financieel oogmerk. Veeleer lijkt er sprake te zijn van een soort ruilhandel.

Deze forums faciliteren niet alleen het uitwisselen van afbeeldingen van seksueel kindermisbruik en informatie met betrekking tot dat kindermisbruik, maar ook de (technische) afscherming ervan. Leden communiceren met elkaar over bepaalde thema's, zoals het type materiaal (bijvoorbeeld jongens versus meisjes, *hardcore* versus *softcore*, *teen* versus *pre-teen*), in informatieve sec-

49 Aanwijzing kinderpornografie 2007, p. 8.

ties (bijvoorbeeld over technieken omtrent computerveiligheid en technische afscherming) en secties met betrekking tot forumbeheer waar administrators nieuwe leden welkom heten en de huisregels uitleggen (Van der Bruggen, 2023). Soms krijgen leden met een hogere status toegang tot verborgen delen op het forum als zij materiaal aanleveren, wat vaak gepaard gaat met een grotere mate van prestige en autoriteit.

Strafbaarstelling

Onder meer het verspreiden, aanbieden, vervaardigen, doorvoeren, uitvoeren, verwerven, in bezit hebben of downloaden van afbeeldingen van seksueel kindermisbruik is strafbaar op grond van het huidige artikel 252 Sr (voorheen art. 240b Sr). Bij die afbeeldingen van seksueel kindermisbruik is sprake van een seksuele gedraging van een persoon die kennelijk de leeftijd van 18 jaar nog niet heeft bereikt. Daarbij geldt een maximumstraf van zes jaar of een geldboete van de vijfde categorie (zie voor een uitgebreide bespreking Van den Hurk et al., 2023).

Casus: afbeeldingen van seksueel misbruik op een dark web forum

Op 3 maart 2020 werd een verdachte veroordeeld voor deelname aan een criminele organisatie. Hij was samen met medeverdachten actief op drie forums en fungeerde zelf als 'hoofdadministrator en hoster' van twee chatrooms.[50] Hij 'promoveerde' bezoekers bijvoorbeeld tot moderator als deze langere tijd 'positief' opvielen. De *staff* van de chatsites hadden verschillende rangen met eigen chatkanalen. Op die kanalen kon men vrijer praten, omdat buitenstaanders minder makkelijk konden meelezen. De leden hielden aantekeningen bij van vergaderingen, wat achteraf bijdroeg aan de bewijsvoering tegen de gebruikers.

De rechtbank ging niet mee in het verweer van de verdediging dat het delen van de tekst en links naar seksueel materiaal van minderjarigen in de chatkanalen geen verspreiding van materiaal van seksueel kindermisbruik behelsde. Ook de waarschuwing op de chatsites dat geen kinderporno mocht worden verspreid, overtuigde de rechters niet omdat uit ander bewijs was af te leiden dat daadwerkelijk illegaal materiaal werd verspreid. In een van de chatrooms werden tussen 26 januari en

50 Zie Rb. Overijssel 3 maart 2020, ECLI:NL:RBOVE:2020:913.

14 juni 2018 2.410 afbeeldingen gedeeld, waarvan er 298 materiaal van seksueel misbruik van minderjarigen betroffen.

Met de Wet seksuele misdrijven die op 1 juli 2024 in werking is getreden is de delictsomschrijving aangepast ten opzichte van het artikel 240b Sr (oud). In het nieuwe artikel 252 Sr is gekozen voor de techniekonafhankelijke formulering 'een visuele weergave van seksuele aard of met een onmiskenbaar seksuele strekking waarbij een kind dat kennelijk de leeftijd van achttien jaren nog niet heeft bereikt is betrokken of schijnbaar is betrokken'.[51] De omschrijving is hiermee beter toegesneden op moderne verschijningsvormen, zoals live streamingbeelden en cloudbestanden met materiaal van seksueel misbruik van kinderen.[52] Het strafmaximum is verhoogd van vier naar zes jaar omdat volgens de wetgever de risico's en schade voor het betrokken kind aanzienlijk zijn toegenomen. Hiermee wordt gedoeld op het feit dat het materiaal tegenwoordig een (nog) veel snellere en bredere verspreiding kent door onder meer het gebruik van sociale media en dat eenmaal verspreide afbeeldingen nauwelijks meer kunnen worden verwijderd en vele malen kunnen worden bekeken.[53]

Met de formulering '*een visuele weergave met een onmiskenbaar seksuele strekking*' doelt de wetgever, in aansluiting bij de jurisprudentie van de Hoge Raad, ook op een afbeelding van een kind in een houding of omgeving die weliswaar op zichzelf of in andere omstandigheden 'onschuldig' zou kunnen zijn, maar die in het concrete geval een onmiskenbaar seksuele strekking heeft, zoals (heimelijke) opnames van zich niet seksueel gedragende kinderen die zich omkleden of douchen. Ook weergaves waarop in het geheel geen gedraging te zien is, zoals close-ups van geslachtsdelen, kunnen een weergave met een onmiskenbare seksuele strekking opleveren.[54]

Ter implementatie van het Cybercrimeverdrag (2001) heeft Nederland ook gedragingen met materiaal van *virtueel* seksueel kindermisbruik strafbaar

51 Zie ook de definitie in art. 239 lid 3 Sr (nieuw): 'In deze titel wordt onder visuele weergave mede verstaan: gegevens die geschikt zijn om een visuele weergave te vormen of een gegevensdrager bevattende gegevens die geschikt zijn om een visuele weergave te vormen.'

52 *Kamerstukken II* 2022/23, 36222, nr. 3, p. 13, p. 57.

53 *Kamerstukken II* 2022/23, 36222, nr. 3, p. 25.

54 *Kamerstukken II* 2022/23, 36222, nr. 3, p. 104.

gesteld. Door het opnemen van de woorden 'schijnbaar betrokken' in de delictsomschrijving hoeft 'het openbaar ministerie niet [meer] de daadwerkelijke betrokkenheid van een echt kind te bewijzen. Voldoende is dat aannemelijk wordt gemaakt dat de afgebeelde persoon op een echt kind lijkt.'[55] Daarbij kan het gaan om afbeeldingen die met behulp van de computer zijn gegenereerd of afbeeldingen van een seksuele gedraging van een kind in de vorm van tekeningen, schilderijen, collages, enzovoort (Van den Hurk et al., 2023). Zulke virtuele afbeeldingen zijn pas strafbaar als het gaat om realistische afbeeldingen, dat wil zeggen 'niet van echt te onderscheiden'.[56]

Aanvankelijk was de lichamelijke schade die het kind werd aangedaan met het vervaardigen van het materiaal en de bescherming tegen het in omloop brengen van dit materiaal, de reden voor de strafbaarstelling van beeldmateriaal van seksueel kindermisbruik. Bij het produceren van materiaal van virtueel seksueel kindermisbruik vindt vanzelfsprekend geen fysiek misbruik van een minderjarige plaats. Bij de strafbaarstelling van dit virtuele materiaal gaat het om bescherming tegen gedrag dat kan worden gebruikt om kinderen aan te moedigen of te verleiden om deel te nemen aan seksueel gedrag of gedrag dat deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert (Koops & Oerlemans, 2019a). Voor de Nederlandse wetgever was ook relevant dat 'ook de vervaardiger van kinderporno waarbij geen (echt) kind is afgebeeld, er immers op uit [is] om kinderpornografisch beeldmateriaal in omloop te brengen dat voor echt doorgaat [en] daarmee een bijdrage [levert] aan de instandhouding van een kinderpornografische markt'.[57]

In 2023 is een nieuwe strafbaarstelling voor 'pedohandboeken' in werking getreden (art. 240c Sr). Het doel is het verwerven, in bezit hebben en anderen bijbrengen van instructies gericht op seksueel misbruik van kinderen, en ook het daarbij voorkomen dat sporen van misbruik achterblijven, strafbaar te stellen met een gevangenisstraf van maximaal vier jaar of een geldboete van de vijfde categorie. Het gaat om voorbereidingshandelingen gericht op het bevorderen van seksueel misbruik door een derde. Kool (2022) stelt dat dit mogelijk al strafbaar is onder artikel 46 Sr. Zij wijst er ook op dat vanuit de Tweede Kamer de vraag werd gesteld of een strafbaarstelling van bezit van pedohandboeken als zodanig, los van de voorbereidingsconstructie, geen betere optie is, omdat verwacht wordt dat het voor de voorbereiding

55 *Kamerstukken II* 2001/02, 27745, nr. 6, p. 8.
56 *Kamerstukken II* 2001/02, 27445, nr. 6, p. 16.
57 *Kamerstukken II* 2001/02, 27445, nr. 6, p. 9.

vereiste opzet tot bewijsproblemen kan leiden, waardoor de reikwijdte van artikel 240c Sr beperkt zal blijken. Ook werden vraagtekens geplaatst ten aanzien van de legaliteit: geeft artikel 240c Sr geen blijk van strafbaarstelling van gedachten, en vormt het geen te vergaande inbreuk op de privacy?

4.6.2 Sexting

De term *sexting* is een samenvoeging van de woorden seks en *texting*. Tegenwoordig heeft het betrekking op het vastleggen van seksuele gedragingen en poses op beeld (bijvoorbeeld met een camera of webcam) en het delen van deze (intieme of seksuele) beelden met een ander door ze met de mobiele telefoon, computer of tablet naar deze ander te verzenden (met wederzijdse instemming – dit wordt ook wel primaire sexting genoemd) (Van Berlo & Ploem, 2018).[58] Wanneer de beelden na ontvangst worden doorgestuurd naar derden wordt gesproken van secundaire sexting (Del Rey et al., 2019).[59] Sexting vindt weliswaar ook plaats tussen meerderjarigen onderling, maar komt vooral veel voor onder jongeren en adolescenten. Het delen van intiem, 'sexy' beeldmateriaal vormt voor jongeren een normaal en belangrijk onderdeel van de seksuele ontwikkeling en de ontdekking van de eigen seksualiteit (Lievens, 2014; Witting, 2019). De gevolgen van sexting hoeven voor betrokkenen dus zeker niet (altijd) negatief of schadelijk te zijn (Gorissen et al., 2020).

Strafbaarstelling

In beginsel is het strafbaar voor minderjarigen die aan sexting doen, om een afbeelding met een seksuele gedraging van zichzelf of de ander te vervaardigen, deze in bezit te hebben of verder te verspreiden. Het gaat dan immers om het vervaardigen, bezitten of verspreiden van 'een visuele weergave met een onmiskenbaar seksuele strekking' als bedoeld in artikel 252 Sr.

Het Openbaar Ministerie stelt in de regel echter geen vervolging in bij consensuele sexting onder jongeren. Dat is anders wanneer er bijvoorbeeld schade is berokkend aan de afgebeelde minderjarige, of wanneer de afbeeldingen bijvoorbeeld na misleiding of onder dreiging tot stand zijn geko-

58 Zie ook Leidraad Afdoening sextingzaken 'Pubers in Beeld', OM en politie, 2017.

59 Met name in niet-Nederlandse literatuur wordt het onderscheid tussen primaire en secundaire sexting gemaakt. Zie bijvoorbeeld: 'Sexting bij jongeren: feiten en cijfers', *Sensoa.be*, geraadpleegd op 12 april 2024.

men.[60] Om tot een goede beoordeling te kunnen komen, worden drie categorieën van sexting onderscheiden:

- Categorie I: er is sprake van (aanwijzingen voor) commerciële elementen, druk, dwang, misleiding, heimelijke opnamen, een afhankelijkheidsrelatie, een slachtoffer jonger dan 12 jaar, een meer dan beperkt leeftijdsverschil (vijf jaar of meer) of een mogelijk ander zedenmisdrijf; indien de verdachte 23 jaar of ouder is, is automatisch sprake van categorie I.
- Categorie II: er zijn aanwijzingen voor andere motieven dan onder categorie I; te denken valt aan pesten, smaad, laster of intimidatie.
- Categorie III: beeldmateriaal lijkt op basis van vrijwilligheid tot stand te zijn gekomen, de betrokkenen zijn beiden minderjarig en het leeftijdsverschil is minder dan vijf jaar, en er is geen sprake van verzwarende omstandigheden zoals beschreven in categorie I en II.

In alle gevallen staat volgens de Leidraad Pubers in Beeld in principe het complete afdoeningsrepertoire ter beschikking: vervolging, OM-afdoening, Halt, reprimande, (voorwaardelijk) sepot of een alternatieve afdoening (Pubers in Beeld, 2017). Gevallen van categorie I-sexting zijn dermate ernstig dat veelal voor vervolging zal worden gekozen. Categorie II-sexting komt ook in aanmerking voor een dagvaarding of voor een HALT-afdoening, (voorwaardelijk) sepot of een OM-afdoening. Voor feiten vallend in categorie III is het strafrecht in principe niet bedoeld – vervolging is dan zeker niet altijd in het belang van de betrokkenen (Aksay & Kouwenberg, 2021).[61]

4.6.3 Misbruik van seksueel beeldmateriaal

Het ongewenst online publiceren van seksueel getinte afbeeldingen of video's van de ex-partner met het doel om deze ex-partner een hak te zetten is al sinds jaar en dag bekend als wraakporno. Daders van wraakporno zijn meestal (dus niet altijd) ex-partners die ten tijde van de relatie seksueel getint beeldmateriaal hebben ontvangen en dit als wraak voor het verbreken van de relatie verspreiden om het slachtoffer publiekelijk te schande te maken of te vernederen. Toch is wraak niet noodzakelijkerwijs het (enige) motief. Vaak wil de dader macht uitoefenen op het slachtoffer, het slachtoffer pesten, vernederen, beledigen of intimideren. Uit onderzoek blijkt dat factoren als het versterken

60 Zie Kristel van Teefelen, 'Jonge dader sexting vaker naar HALT', *Trouw.nl*, 13 april 2017. Aanwijzing kinderpornografie 2016 en Leidraad Afdoening sextingzaken 'Pubers in Beeld', OM en politie, 2017.

61 Zie voor nadere uitwerking Leidraad Afdoening sextingzaken 'Pubers in Beeld', OM en politie, 2017.

van vriendschappen tussen daders, het reguleren van elkaars seksuele gedrag of het vergroten van de eigen populariteit ook meespelen (Gorissen et al., 2020). De term 'wraakporno', hoewel ingeburgerd als parapluterm voor het bedoelde fenomeen, dekt de brede lading van verschijningsvormen als *online shaming*, het ongewenst publiceren van seksueel beeldmateriaal, of het maken of verspreiden van pornografische *deepfakes*, waarop wij hieronder in gaan, dus niet meer volledig.

In deze laatste gevallen spreken we dan eerder van misbruik van seksueel beeldmateriaal, online shaming of – zoals het CBS het noemt – *shamesexting*. Uit de Veiligheidsmonitor (2024) blijkt dat in 2023 0,4% van de Nederlanders te maken heeft gehad met shamesexting, dat wordt gedefinieerd als 'het verspreiden van naaktfoto's of -filmpjes of hiermee dreigen'.[62] Dit misbruik van seksueel beeldmateriaal kan heel grootschalig plaatsvinden, met name bij het online shamen in zogenoemde exposegroepen, waarbij foto's van (vaak vrouwelijke) slachtoffers, dikwijls voorzien van persoonlijke informatie en persoonsgegevens, worden gepubliceerd en/of gedeeld. De rechtbank Midden-Nederland overwoog bijvoorbeeld in een zaak hoe naaktfoto's, samen met het profiel van Instagram en Snapchat van het slachtoffer werden gedeeld op een Telegram-kanaal met 88.215 leden.[63]

Ten slotte wijzen wij hier nog op een vorm van misbruik van seksueel beeldmateriaal die in de nabije toekomst ongetwijfeld in betekenis gaat toenemen: seksuele *deepfakes* (Goudsmit Samaritter et al., 2023; Van der Sloot et al., 2021). De term 'deepfake' is een samentrekking van *deep* en *fake*. 'Deep' verwijst naar *deep learning*- en *machine learning*-algoritmen die worden gebruikt om het materiaal te maken, terwijl 'fake' de inherente kunstmatigheid van het materiaal benadrukt. De onderliggende technologie van deze software voor het maken van deepfakes wordt *generative adversarial networks* genoemd (zie Goodfellow et al., 2020). Deze technologie werd onmiddellijk gebruikt (misbruikt) om niet-consensuele seksuele deepfakes te maken van beroemdheden (McCosker, 2022).

62 CBS, Veiligheidsmonitor 2023, p. 52.

63 Rb. Midden-Nederland 1 februari 2022, ECLI:NL:RBMNE:2022:294. De rechtbank veroordeelde de verdachte overigens voor dwang (art. 284 Sr) (met bedreiging van enige andere feitelijkheid gericht tegen die ander, dwingen iets te dulden (in dit geval het niet blokkeren van de dader)) en het zonder toestemming openbaar maken van afbeeldingen van seksuele aard (art. 139h Sr).

Casus: deepnudes op Reddit

In 2017 werden de gezichten van Amerikaanse beroemdheden, zoals Taylor Swift en Gal Gadot, op de lichamen van pornoactrices gezet (een *face swap* genoemd). Deze video's werden voor het eerst verspreid op het platform Reddit. Reddit-gebruiker '/u/deepfakes' was een gebruiker van de subreddit (een soort internetforum) '/r/deepfakes'. Deze subreddit was gewijd aan het delen van niet-consensuele seksuele deepfakes en won snel aan populariteit.[64]

In februari 2018 verbood Reddit deze seksuele deepfake-subreddit en dit voorbeeld werd gevolgd door andere populaire platforms, zoals Discord (een chatplatform), Pornhub (een pornografische website), X (voorheen Twitter, een microblogdienst) en Meta (voorheen Facebook, een sociale-mediadienst).[65] Onderzoek toont aan dat het aantal niet-consensuele seksuele deepfakes snel toeneemt en voornamelijk gericht is op vrouwen als onderwerp van seksuele deepfakes (Flynn et al., 2022; Pascale, 2023).

In 2023 werden *generative AI-apps* zeer populair. Met deze apps wordt 'nieuwe' content gegenereerd en niet slechts materiaal gemanipuleerd. Door middel van een opdracht (een *prompt*) krijgt de software een instructie om tekst, afbeeldingen, audio of video te genereren. Het misbruik van deze apps werd onder andere duidelijk toen deepfakes van Taylor Swift op 25 januari 2024 werden verspreid op het platform X. Enkele afbeeldingen kregen 45 miljoen *views* en 24.000 reposts. Het materiaal bleef 17 uur online, totdat het werd verwijderd door het platform.[66]

64 S. Cole, 'AI-assisted Fake Porn Is Here and We're All Fucked', *Motherboard*, 11 december 2017.

65 A. Hern, '"Deepfake" face-swap porn videos banned by Pornhub and Twitter', *The Guardian*, 7 februari 2018 en D. Hawkins, 'Reddit bans "deepfakes" pornography using the faces of celebrities such as Taylor Swift and Gal Gadot', *The Washington Post*, 8 februari 2018.

66 J. Weatherbed, 'Trolls have flooded X with graphic Taylor Swift AI fakes', *The Verge*, 25 januari 2024. Zie ook voor een Nederlands voorbeeld: 'Geschokte reacties na opduiken BN'ers en politici in met AI gemanipuleerde pornovideo's', *RTL Nieuws*, 19 maart 2024.

Strafbaarstelling

Het misbruik van seksueel beeldmateriaal is sinds 1 januari 2020 strafbaar gesteld, aanvankelijk in artikel 139h Sr (oud), en sinds 2024 in artikel 254ba Sr.[67] Deze bepaling stelt verschillende facetten van het (al dan niet online) misbruiken van seksueel beeldmateriaal strafbaar, zoals het opzettelijk en wederrechtelijk vervaardigen van een visuele weergave van seksuele aard van iemand (lid 1 sub a), of de beschikking hebben over een dergelijke visuele weergave terwijl de verdachte weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een wederrechtelijke gedraging is verkregen (lid 1 sub b).

Ook het openbaar maken, bijvoorbeeld het op internet zetten van een dergelijke visuele weergave (al dan niet met persoonsgegevens daarbij (exposen)), is strafbaar, wanneer de verdachte weet of redelijkerwijs moet vermoeden dat deze visuele weergave van seksuele aard opzettelijk en wederrechtelijk is verkregen (lid 2 sub a) of wanneer die weet dat openbaarmaking nadelig kan zijn voor het slachtoffer (lid 2 sub b).

Uit de vrij uitgebreide jurisprudentie over misbruik van seksueel beeldmateriaal sinds 2020 rijst een gevarieerd beeld op van bijvoorbeeld daders die heimelijk filmpjes maken in kleedhokjes van een zwembad of sporthal, of seksuele video's en foto's van een ex-vriendin naar familieleden van het slachtoffer sturen, of met behulp van een verborgen camera heimelijk opnames maken in de slaapkamer van het slachtoffer.[68] In het vonnis dat betrekking had op de pornografische deepfake van de presentatrice Sijtsma heeft de rechtbank geoordeeld dat het vervaardigen en vervolgens openbaar maken van een deepfake video van het slachtoffer binnen de reikwijdte van artikel 139h Sr (oud) valt.[69]

Het misbruik van seksueel beeldmateriaal is onder omstandigheden ook op grond van andere delicten strafbaar (Banning et al., 2023). Denk daarbij bijvoorbeeld aan smaadschrift (art. 261 Sr), waarbij iemands eer of goede naam wordt aangerand met het kennelijke doel daaraan ruchtbaarheid te geven en

67 *Kamerstukken II* 2022/23, 36222, nr. 20.

68 Hof Amsterdam 29 september 2022, ECLI:NL:GHAMS:2022:2797, Hof Den Haag 23 december 2021, ECLI:NL:GHDHA:2021:2926, Rb. Amsterdam 26 augustus 2021, ECLI:NL:RBAMS:2021:4470.

69 Rb. Amsterdam 2 november 2023, ECLI:NL:RBAMS:2023:6923, *Computerrecht* 2024/8, m.nt. J.J. Oerlemans & dr. S. Royer (*seksuele deepfake*). Over het voorval en de impact op haar en haar omgeving heeft zij de documentaire 'Welmoed en de sexfakes' (2022) gemaakt.

aan identiteitsfraude (art. 231b Sr) (Goudsmit Samaritter et al., 2023). Van der Hof (2016) legt uit dat daarvan bijvoorbeeld sprake kan zijn als bijvoorbeeld een foto van een ex online wordt geplaatst met daarbij begeleidende teksten via de chat, forums of sociale media.[70]

Vanaf december 2020 is een nieuwe strafvorderingsrichtlijn van kracht rondom misbruik van seksueel beeldmateriaal.[71] In deze richtlijn wordt ten aanzien van misbruik van seksueel beeldmateriaal (van meerderjarigen door meerderjarigen) onderscheid gemaakt tussen drie categorieën: (1) (dreigen met) verspreiding, (2) opzettelijke, wederrechtelijke vervaardiging, en (3) passief bezit (materiaal is toegestuurd en door verdachte niet verder verspreid). De drie delictscategorieën kennen in veel gevallen een strafmaatbandbreedte. Het begint met het eenmalig plegen van het verspreiden van beeldmateriaal door één meerderjarige verdachte, zonder dat er sprake is van (relevante) recidive. Naarmate er sprake is dwang of dreiging wordt de eis zwaarder. De straf(eisen) variëren van een geldboete of een taakstraf tot een onvoorwaardelijke gevangenisstraf van drie tot twaalf maanden.[72]

4.6.4 Sextortion

Sextortion is een samenvoeging van de Engelse woorden sex en *extortion* en verwijst naar het gebruik van seksueel getint beeldmateriaal als chantagemiddel (Wolak & Finkelhor, 2011). Van sextortion is bijvoorbeeld sprake wanneer het slachtoffer eerst wordt verleid om een naaktbeeld te tonen (bijvoorbeeld via de webcam) of op te sturen, waarna deze webcamopnamen of beelden worden gebruikt om het slachtoffer te dwingen tot meer – eventueel steeds verdergaande – seksuele handelingen voor de webcam, en er gedreigd wordt dat de beelden via internet zullen worden verspreid. Ook komt voor dat het slachtoffer wordt gedwongen tot het betalen van geld of het verlenen van andere (seksuele) diensten. Het verschil met ongewenste sexting en wraakporno is dat dreiging gebruikt wordt om een slachtoffer ertoe te dwingen iets te doen, zelfs als het verspreiden van het beeldmateriaal nooit plaatsvindt (Wolak et al., 2018).

70 Zie verder Richtlijn strafvordering misbruik seksueel beeldmateriaal 2020.

71 Richtlijn voor strafvordering misbruik seksueel beeldmateriaal, *Stcrt.* 2020, 62637.

72 Richtlijn voor strafvordering misbruik seksueel beeldmateriaal, *Stcrt.* 2020, 62637, p. 2-3.

Casus: Aydin C.

Aydin C., ook wel bekend als de 'webcamafperser', kreeg internationale bekendheid door de zelfdoding van de 15-jarige Canadese Amanda Todd in 2012.[73] Zij was als gevolg van C.'s praktijken dermate tot wanhoop gedreven dat ze besloot een einde aan haar leven te maken. Haar YouTube-filmpje hierover kreeg wereldwijde bekendheid.

Aydin C. werd verdachte in een Nederlandse strafzaak nadat de beveiligingsafdeling van Facebook een rapport naar Engelse autoriteiten had doorgestuurd over een mogelijke kindmisbruiker. Na enige tijd brachten de Engelsen de Nederlandse autoriteiten op de hoogte. Aydin C. ging geraffineerd te werk. Hij gebruikte vele aliassen op Facebook om 34 minderjarige vrouwen en vijf volwassen mannen te verleiden blootvideo's of foto's van zichzelf te maken waarna hij ze afperste en dwong hem van nieuw materiaal te voorzien. Daarbij deed hij zich voor als minderjarige jongen. Aydin C. gebruikte ook beelden voor chantage van masturberende mannen die aan het webcammen waren met – zo dachten ze – een minderjarige jongen. Bij niet-betaling zou de verdachte de beelden verspreiden onder vrienden en familie. Hij verborg zijn IP-adres met een *virtual private network* (VPN)-verbinding (zie hoofdstuk 9) en misbruikte paspoorten van anderen voor de registratie bij de online betalingsdienst Skrill. Hij gebruikte de betalingsdienst Western Union voor het ophalen van de bedragen (in totaal meer dan € 30.000) die hij door webcamafpersing had verkregen.[74]

In 2018 heeft het Hof Amsterdam Aydin C. veroordeeld tot tien jaar en acht maanden gevangenisstraf voor de 'sextortion' van zijn slachtoffers.[75] De Canadese straf die hij kreeg opgelegd voor het afpersen en intimideren van Amanda Todd bedroeg dertien jaar en is door de Nederlandse rechter omgezet in (nog eens) zes jaar.[76]

73 Zie 'The Sextortion of Amanda Todd', *CBC*, 15 november 2013 en 'De dood van Amanda Todd', *Zembla*, 4 december 2014 (documentaire).

74 Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, m.nt. J.J. Oerlemans (*Aydin C.*-zaak).

75 Hof Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4620.

76 Rb. Amsterdam 23 december 2023, ECLI:NL:RBAMS:2023:8234.

Strafbaarstelling

In de Aydin C.-zaak werden de gedragingen van Aydin C. aangemerkt als (online) aanranding (art. 246 Sr) en afdreiging (art. 318 Sr) omdat de slachtoffers vaak niet de mogelijkheid hadden om te verhinderen dat de dader de afbeeldingen verspreidde en zich daarom gedwongen voelden om toe te geven aan de dader. In dat geval is er sprake van (poging tot) aanranding op afstand. Het is voor aanranding dus niet vereist dat er fysiek contact is tussen de dader en het slachtoffer; aanranding kan onder deze omstandigheid ook op afstand plaatsvinden.[77]

Van afdreiging (art. 318 Sr) is sprake wanneer de afbeeldingen of video's later tegen het slachtoffer worden gebruikt om deze te chanteren. Daarnaast kan sprake zijn van afpersing (art. 317 Sr) als de afperser gericht is op het verkrijgen van geld of meer seksueel getint materiaal. In situaties waarbij de seksuele gunsten *hands-on* moeten plaatsvinden, kan sprake zijn van dwang, zoals omschreven in artikel 284 Sr (Cleiren et al., 2019; Gorissen et al., 2020; Ten Voorde, 2017a).[78]

In een vergelijkbare zaak waarbij acht jonge verdachten van 15 tot 18 jaar zich hadden schuldig gemaakt aan het chanteren van leeftijdsgenoten werd hun, naast deelname aan een criminele organisatie en witwassen, ook (poging tot) afdreiging ten laste gelegd.[79] Hun slachtoffers, van wie de jongste 14 jaar oud was, waren vooral jongens met wie de daders contact legden op sociale media als Instagram en Snapchat door zich voor te doen als meisjes. Ze vroegen hun slachtoffers om naaktfoto's van zichzelf te sturen waarna ze dreigden de beelden openbaar te maken als de slachtoffers niet betaalden. Tientallen, wellicht meer dan honderd, slachtoffers zijn op deze wijze afgeperst met hun eigen naaktbeelden waarmee de daders in totaal 100.000 euro hebben verdiend.[80]

77 Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, m.nt. J.J. Oerlemans (*Aydin C.*-zaak) en Hof Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4620, *Computerrecht* 2019/52, m.nt. M.H.G.M. van der Linden.

78 Dwang is het 'door bedreiging met geweld of andere feitelijkheden dwingen iets te doen, te laten of te dulden'.

79 Rb. Den Haag 6 januari 2021, ECLI:NL:RBDHA:2021:28.

80 R. Andringa, 'Jonge criminelen streken ton op door chantage met naaktfoto's', *NOS.nl*, 2 november 2019.

4.6.5 Online grooming en sexchatten

Online *grooming* kan worden omschreven als het online inkapselen van een minderjarige met het oogmerk seksueel misbruik te plegen of kinderpornografische afbeeldingen te produceren (Lindenberg & Van Dijk, 2016). Het fenomeen wordt ook wel digitaal of 'online kinderlokken' genoemd (Jonker et al., 2017; De Hingh, 2018).

In de wetenschappelijke literatuur wordt grooming soms beschreven als een (langdurig) proces waarin de *groomer* een reeks elkaar in tijd opvolgende fases doorloopt (O'Connell, 2003). Deze fases hebben betrekking op respectievelijk vriendschapsvorming, relatievorming, risicobeoordeling, exclusiviteit en de seksuele fase. Uit onderzoek komt echter ook naar voren dat het verloop van online grooming sterk kan variëren en dat de tijd die groomers besteden aan de verschillende fases eveneens erg kan verschillen (sommige groomers gaan bijvoorbeeld vrijwel direct over tot de seksuele fase) (Gorissen et al., 2020).

Het algemene beeld is wel dat de potentiële groomer na de eerste kennismaking met een minderjarige door (veelvuldig) chat- of e-mailcontact langzaam het vertrouwen van het kind wint, het verleidt tot het delen van bepaalde intimiteiten en het aldus vatbaar maakt voor seksueel misbruik in de fysieke wereld.[81] Grooming-gedrag bestaat dus in hoofdzaak uit communicatie en uit dat taalgebruik – bijvoorbeeld seksuele toespelingen in de chat-, sms- of e-mailgesprekken – zal veelal (moeten) blijken dat het de dader uiteindelijk te doen is om het plegen van seksueel misbruik in de echte wereld (De Hingh, 2018; 2023).

Strafbaarstelling

Online grooming staat sinds juli 2010 in artikel 248e Sr (oud) waarmee de Nederlandse wetgever uitvoering gaf aan de implementatie van artikel 23 van het Verdrag van Lanzarote.[82] Sinds de inwerkingtreding van het Wetsvoorstel seksuele misdrijven in 2024 is grooming strafbaar gesteld in artikel 251 Sr lid 1 sub c. Het wordt beschouwd als een voorbereidingsdelict, wat betekent dat het strafbaar is gesteld wanneer iemand aan een kind jonger dan 16 jaar een (concrete) ontmoeting voorstelt voor seksuele doeleinden (namelijk met het oogmerk om in tweede instantie ontuchtige handelingen met dat kind te

81 *Kamerstukken II* 2008/09, 31810, nr. 3, p. 6-7.

82 Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen uitbuiting en seksueel misbruik (*Trb.* 2008, 58), in werking getreden per 1 januari 2010.

plegen of afbeeldingen van seksueel misbruik te vervaardigen) en vervolgens 'enige handeling onderneemt tot het verwezenlijken van die ontmoeting'.[83]

Onder het 'ondernemen van enige handeling ter verwezenlijking van de ontmoeting' kan, zo blijkt uit de wetsgeschiedenis, van alles worden verstaan: het aankomen op de voorgestelde ontmoetingslocatie, het toesturen van een treinkaartje of het doorgeven van een routebeschrijving, bijvoorbeeld, worden beschouwd als handelingen ter verwezenlijking van de voorgestelde ontmoeting. Maar ook 'het er bij het slachtoffer in chats en sms-berichten herhaaldelijk op aandringen dat er snel *een* ontmoeting moet plaatsvinden en daarbij het slachtoffer onder druk zetten', plus 'het geven van een telefoonnummer aan het slachtoffer' was in 2014 naar het oordeel van de Hoge Raad voldoende om te kunnen spreken van online grooming in de zin van artikel 248e Sr (oud), het huidige artikel 251 Sr lid 1 sub c (De Hingh, 2018).[84]

Casus: Sweetie 2.0 en de lokpuber

Met de Wet computercriminaliteit III werd in 2019 het wetsartikel 248e Sr (oud) uitgebreid.[85] Vanaf dat moment kon iemand zich ook schuldig maken aan online grooming door een ontmoeting voor te stellen aan een zogenoemde 'lokpuber'. Deze lokpuber kan bijvoorbeeld een politiebeambte zijn die zich met een fake online account voordoet als een persoon die de leeftijd van 16 jaar nog niet heeft bereikt, maar ook een bezorgde ouder, of een willekeurige andere volwassene, en ook zogenoemde 'pedohunters' die het heft in eigen hand willen nemen.[86]

Sweetie 2.0 was een chatbot met het uiterlijk van een Filipijns meisje. Deze virtuele lokpuber was door de kinderrechtenorganisatie Terres des Hommes in 2013 ontwikkeld in hun strijd tegen het fenomeen van webcamseks met minderjarigen in de Filipijnen. Met deze virtuele

83 *Kamerstukken II* 2008/09, 31810, nr. 3, p. 9. Zie ook Hof Arnhem 15 september 2011, ECLI:NL:GHARN:2011:BT1553.

84 HR 11 november 2014, ECLI:NL:HR:2014:3140.

85 Art. 248e Sr: 'iemand die zich, al dan niet met een technisch hulpmiddel, *waaronder een virtuele creatie van een persoon die de leeftijd van zestien jaren nog niet heeft bereikt*, voordoet als een persoon die de leeftijd van zestien jaren nog niet heeft bereikt' [cursivering toegevoegd].

86 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 71.

lokpuber kon men mannen die zich aan deze webcamseks schuldig maakten op heterdaad betrappen (Van der Hof et al., 2019). Ongeveer 20.000 mannen uit zo'n 71 landen zochten contact met Sweetie 2.0. In de tien weken tijd dat het project liep konden op basis van persoonlijke gegevens en Facebookgegevens zo'n duizend verdachten worden geïdentificeerd en worden overgedragen aan de opsporingsautoriteiten van hun eigen land.[87]

Geïnspireerd door het virtuele meisje Sweetie is in 2019 via een amendement de zogenoemde 'virtuele creatie van een persoon die de leeftijd van zestien jaren nog niet heeft bereikt' ook in het toenmalige artikel 248e van het Nederlandse Wetboek van Strafrecht terechtgekomen waardoor sindsdien het groomen van een *virtuele* lokpuber (of chatbot) onder omstandigheden kan leiden tot een strafbaar feit (Lindenberg, 2016).

Met de Wet seksuele misdrijven die op 1 juli 2024 in werking is getreden, wordt in één nieuw wetsartikel (art. 251 Sr) de strafbaarstelling van online grooming samengevoegd met het zogenoemd 'seksueel corrumperen van kinderen' en het sekschatten met kinderen. Seksueel corrumperen (art. 251 lid 1 sub b) wil zeggen: kinderen blootstellen aan een seksuele handeling of een visuele weergave van seksuele aard. Onder sekschatten (art. 251 lid 1 sub a) verstaat de wetgever 'het op indringende en niet leeftijdsconforme wijze mondeling of schriftelijk seksualiserend communiceren met kinderen'.[88] Bij dat laatste gaat het dus om gedragingen waarbij (nog) geen sprake is van een ontmoetingsvoorstel of het verrichten van enige handeling ter verwezenlijking van die ontmoeting (zoals bij online grooming), maar waarbij uitsluitend indringend seksualiserend wordt gecommuniceerd met een 16-minner (De Hingh, 2023). De wetgever geeft aan dat strafbaarstelling van sekschatten wenselijk was, omdat de seksualiserende benadering van kinderen schadelijk is en het een drempelverlagend effect heeft richting seksueel misbruik.[89]

Ook bij de opsporing van het seksueel corrumperen van kinderen en het sekschatten met kinderen kan gebruikgemaakt worden van een lokpuber

87 F. Huiskamp, 'Voor het eerst man veroordeeld vanwege chatten met virtuele meisje sweetie', *NRC*, 21 oktober 2014.

88 *Kamerstukken II* 2022/23, 36222, nr. 3, p. 25.

89 *Kamerstukken II* 2022/23, 36222, nr. 3, p. 13.

– 'een persoon die zich voordoet als een kind beneden de leeftijd van zestien jaren' – al dan niet in de vorm van een chatbot (oftewel een virtuele creatie). Een opvallende wijziging in artikel 251 Sr ten opzichte van de oude wetsbepalingen is dat de aanduiding van het online communicatiemiddel waarmee de strafbare feiten (met name relevant bij sekschatten en groomen) worden gepleegd is komen te vervallen. Het lijkt een weloverwogen beslissing te zijn van de wetgever om ook de *offline* varianten van deze delicten strafbaar te stellen. Ruim tien jaar nadat in Nederland naast de fysieke kinderlokker ook een digitale kinderlokker werd geïntroduceerd, heeft de Wet seksuele misdrijven in 2024 de *offline sexchatter* en de *offline groomer* in het leven geroepen (De Hingh, 2023).

4.7 Online uitingsdelicten

De ontwikkeling van sociale media en de toename van online inhoud die gebruikers zelf creëren (*user generated content*) leiden ook tot een toename van uitingsdelicten. Het CBS rapporteert in de Veiligheidsmonitor 2024 dat in 2023 3% van de geënquêteerden slachtoffer zegt te zijn geweest van online bedreiging en intimidatie. Begrippen als online bedreiging en online intimidatie worden vaak door elkaar gehaald. Ook wordt wel de overkoepelende term 'online haatspraak' (*hate speech* in het Engels) gebruikt (Van Huijstee et al., 2021). Wij gebruiken de term 'online uitingsdelicten', waarbij wij bij de strafbaarstellingen aansluiten. Uitingsdelicten zijn uitingen van personen die wegens hun inhoud in het Wetboek van Strafrecht strafbaar zijn gesteld (Janssens & Nieuwenhuis, 2019) en zijn meestal gericht op gender, religie, ras en fysieke of lichamelijke beperkingen (Chetty & Alathur, 2018). Onder uitingen wordt verstaan: het kenbaar maken van gedachten of gevoelens, op welke wijze dan ook.[90]

Volgens het OM (OM 2022) is de instroom van het delict eenvoudige belediging verreweg het grootst (184 in 2022), op afstand gevolgd door bedreiging (art. 285 Sr, met 35 in 2022). Dat zijn vooral zaken over belediging van ambtenaren in functie, want die worden standaard gemeld en vervolgd. Burgers krijgen in dat geval vaak een strafbeschikking opgelegd en als ze het daar niet mee eens zijn worden ze betrokken in een strafrechtelijke procedure. In andere beledigingszaken gaat het OM in veel gevallen niet tot vervolging over, omdat het OM het strafrecht niet ziet als het juiste middel om op te treden tegen belediging. Overings liggen civiele maatregelen meer voor de hand dan

90 Rb. Rotterdam 12 juli 2022, ECLI:NL:RBROT:2022:5674, r.o. 4.3.1.

de inzet van het strafrecht, dat immers een ultimum remedium is (Kesar, 2018). Door middel van een proces kunnen slachtoffers schadevergoeding, rectificatie of verwijdering van het materiaal eisen. Het Europees Hof voor de rechten van de Mens (EHRM) benadrukt ook in jurisprudentie dat de vervolging van uitingsdelicten in het strafrecht beperkt zou moeten zijn tot noodzakelijke, serieuze zaken.[91] Met betrekking tot discriminatie rapporteert het OM dat de meeste feiten (144 in 2022) betrekking hadden op de discriminatiegrond ras, antisemitisme en hetero- of homoseksuele gerichtheid (OM, 2022). Het overgrote deel van alle ingekomen specifieke discriminatiefeiten had betrekking op groepsbelediging.

In de literatuur komt steeds meer aandacht voor uitingsdelicten zoals haatzaaien (vaak geschaard onder de noemer *cyber violence* of *online hate speech*, waarbij onder meer gekeken wordt naar de aard en omvang van haatzaaien, maar ook naar wat online haatzaaien wezenlijk anders maakt dan offline haatzaaien (zie bijvoorbeeld Bakalis, 2018; Brown, 2018; Chetty & Alathur, 2018); Citron, 2014; Mathew et al., 2019). In het kader van dit laatste wordt bijvoorbeeld gekeken naar de rol van anonimiteit en online disinhibitie, het feit dat daders vanwege de anonimiteit sneller overgaan tot grof taalgebruik en haat (Suler, 2004, zie verder hoofdstuk 8). Ook is er aandacht voor de verwevenheid tussen de digitale en fysieke wereld. De voedingsbodem voor een conflict kan bijvoorbeeld tijdens het chatten of op een forum op internet ontstaan, maar uiteindelijke resulteren in een face-to-face bedreiging. Andersom kan in de fysieke wereld een conflict tussen mensen ontstaan, en dan langs de digitale weg resulteren in uitingsdelicten zoals smaad of bedreiging (Huijstee et al., 2021, Van Wilsem, 2010).

Hoewel het duidelijk is wat er onder uitingsdelicten wordt verstaan is het bepalen van de strafbaarheid ervan minder evident. Daarom wordt allereerst nader ingegaan hoe het strafbaar stellen en vervolgen voor uitingen op gespannen voet kunnen staan met de vrijheid van meningsuiting. Daarna worden enkele specifieke strafbaarstellingen besproken.

4.7.1 Uitingsdelicten en de vrijheid van meningsuiting

Telkens als een uiting van een persoon strafbaar wordt gesteld, maakt dat een inbreuk op de vrijheid van meningsuiting, zoals vastgelegd in artikel 7 Grondwet en artikel 10 Europees Verdrag voor de Rechten van de Mens (EVRM).

91 EHRM 20 november 2006, nr. 47579/99, ECLI:CE:ECHR:2006:0420JUD004757999 (*Raichinov/Bulgarije*), par. 46 en 50.

Een inbreuk op de vrijheid van meningsuiting vormt een probleem, omdat dit grondrecht wordt gezien als een voorwaarde voor het functioneren van een democratie en voor de uitvoering van een effectief systeem van mensenrechten.[92] Een te ruime strafbaarstelling van uitingsdelicten kan bovendien leiden tot misbruik en (zelf)censuur uit vrees voor strafrechtelijke consequenties.[93] Volgens het EHRM dient er in een democratie in beginsel ook ruimte te zijn voor uitlatingen die kwetsen, shockeren of verontrusten.[94] Tegelijkertijd signaleert het EHRM ook het gevaar van een snelle verspreiding van bijvoorbeeld haatzaaien (hate speech) en opruiing via internet.[95]

De toegang tot informatie via internet vormt een onderdeel van het recht op de vrijheid van meningsuiting, naast het publiceren van informatie.[96] Het EHRM ziet een belangrijke rol voor het internet weggelegd om de toegang tot nieuws voor het publiek te verbeteren en de verspreiding van informatie in het algemeen te vergemakkelijken.[97] Het beperken daarvan, bijvoorbeeld door een website te blokkeren, vormt daarmee een beperking van de vrijheid van meningsuiting.[98]

Slechts onder voorwaarden mag een uiting strafbaar worden gesteld. Als het EHRM vaststelt dat er sprake is van een beperking van artikel 10 EVRM, volgt telkens de volgende 'drietrapsraket': (1) is de beperking bij wet voorzien?; (2) dient zij een van de in artikel 10 lid 2 EVRM genoemde doelen?; en (3) is zij

92 Zie bijvoorbeeld EHRM 7 december 1976, nr. 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372 (*Handyside/Verenigd Koninkrijk*), par. 49, EHRM 15 oktober 2015, nr. 27510/08, ECLI:CE:ECHR:2015:1015JUD002751008, (*Perínçek/Zwitserland*), par. 196; en EHRM 26 maart 2016, nr. 56925/08, ECLI:CE:ECHR:2016:0329JUD005692508 (*Bédat/Zwitserland [GK]*), par. 48.

93 Dit wordt ook het 'chilling effect' genoemd.

94 EHRM 7 december 1976, nr. 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372 (*Handyside/Verenigd Koninkrijk*), par. 49.

95 EHRM 16 juni 2015, nr. 64569/09, ECLI:CE:ECHR:2015:0616JUD006456909 (*Delfi/Estland*), par. 110.

96 EHRM 1 december 2015, nrs. 48226/10 en 14027/11, ECLI:CE:ECHR:2015:1201JUD 004822610 (*Cengiz/Turkije*), par. 52-54. Zie ook EHRM 16 december 1012, nr. 3111/10, ECLI:CE:ECHR:2012:1218JUD000311110 (*Ahmet Yildirim/Turkije*), par. 50.

97 Zie bijvoorbeeld EHRM 16 juni 2015, nr. 64569/09, ECLI:CE:ECHR:2015:0616 JUD006456909 (*Delfi/Estland*), par. 133.

98 EHRM 1 december 2015, nrs. 48226/10 en 14027/11, ECLI:CE:ECHR:2015:1201JUD 004822610 (*Cengiz/Turkije*), par. 59-67. Zie ook T.E. McGonagle, in zijn annotatie bij: EHRM 23 juni 2020, nr. 20159/15, ECLI:CE:ECHR:2020:0623JUD002015915 (*Bulgakov/Rusland*) en EHRM 23 juni 2020, nr. 10795/14, ECLI:CE:ECHR:2020:0623 JUD001079514 (*Kharitonov/Rusland*), *EHRC Updates* 2020, 'Court stands firm on excessive nature of IP-address blocking'.

noodzakelijk in een democratische samenleving? Binnen de derde stap valt ook een afweging van belangen en de toepassing van het proportionaliteitsbeginsel (ook wel evenredigheidsbeginsel genoemd). Deze drietrapsraket komt ook vaak terug in Nederlandse uitspraken met betrekking tot uitingsdelicten (Janssens & Nieuwenhuis, 2019 en De Ruiter & Velleman, 2023).

4.7.2 Strafbaarstelling van uitingen

Uitingsdelicten kunnen gecategoriseerd worden in: strafbare belediging, smaad, laster, discriminatie, opruiing, bedreiging en doxing. Bij strafbare belediging gaat het in de kern om uitingsdelicten waarbij door middel van een uiting door iemand, een persoon in een ongunstig daglicht wordt gesteld en wordt aangetast in zijn eer en goede naam.[99] Die eer of goede naam van een persoon moet worden opgevat als de erkenning van de morele integriteit van een persoon in een openbare ruimte (Janssens & Nieuwenhuis, 2019).

Het antwoord op de vraag of een uiting strafbaar is, is niet altijd eenvoudig te beantwoorden. Dat komt onder meer omdat de concrete invulling van de gedraging afhankelijk is van de 'tijdgebonden maatschappelijke opvattingen' (De Hullu, 2018). De vraag of een uiting strafbaar is, moet aan de hand van een concrete situatie worden beantwoord. Bovendien kunnen het algemeen belang en de vrijheid van meningsuiting prevaleren boven de vermeende strafbaarheid van de uiting. De context kan ervoor zorgen dat een op zichzelf beledigende uiting toch bescherming verdient, bijvoorbeeld als de uiting een bijdrage levert aan het maatschappelijke debat. De pleger van smaad, smaadschrift of laster moet dan te goeder trouw kunnen aannemen dat zijn bewering waar is én dat het algemeen belang de beschuldiging eist (art. 261 lid 3). Als het belang van de vrijheid van meningsuiting van een persoon prevaleert boven het belang van het slachtoffer van de belediging, moet vrijspraak of ontslag van alle rechtsvervolging volgen.

Bij strafbare belediging is telkens vereist dat de uiting 'in het openbaar' plaatsvindt. De Hoge Raad heeft 'zich in het openbaar uitlaten' gedefinieerd als het 'ter kennis van het publiek brengen'.[100] In een digitale context is die definitie niet altijd duidelijk. Dat levert bijvoorbeeld de vraag op of het delen van een bericht of afbeelding in een communicatieapp of sociale media 'openbaar' is of niet. Van openbaarheid was *geen* sprake in een zaak waarin een

99 HR 30 oktober 2001, ECLI:HR:2001:AB3143 en HR 29 maart 2016, ECLI:NL:HR:2016:510.

100 HR 22 april 2014, ECLI:NL:HR:2014:952.

verdachte in een WhatsAppgroep van veertien actieve deelnemers opruiende berichten had geplaatst.[101] Dat zal anders zijn in openbare Telegramgroepen.[102] Ook beledigende uitlatingen op een afgeschermd profiel met 10 à 12 vrienden op een sociale mediadienst (alleen toegankelijk voor vrienden), beschouwde het Hof Den Bosch bijvoorbeeld niet als 'openbaar', voor zover het aantal vrienden 'gering' blijft.[103] Kortom, de eis van openbaarheid moet worden getoetst aan de hand van de omstandigheden van het geval. De Hoge Raad heeft wel een aantal omstandigheden genoemd aan de hand waarvan kan worden beoordeeld of een uiting aan het publiek ter kennis is gebracht.[104] Het gaat daarbij in de kern om (a) de omvang van de kring van personen tegenover wie de uiting is gedaan, (b) de mate van onderlinge verbondenheid in de kring, en (c) de inhoud, vorm en wijze waarop de uiting is gedaan (De Ruiter & Velleman, 2023, p. 94).

Tot slot is het belangrijk te benoemen dat de delicten belediging, smaad en laster zogenoemde 'klachtdelicten' betreffen. Dat betekent dat een persoon eerst aangifte bij de politie moet doen met een verzoek tot vervolging, voordat het OM vervolging kan instellen (art. 164 Sv). De uitzondering daarop is, kortgezegd, als het delict strafbare belediging is gericht tegen het openbaar gezag, een openbaar lichaam of een openbare instelling of een ambtenaar tijdens of ter zake van de uitoefening van zijn taak (art. 269 Sr).

Smaad en laster

Bij het delict smaad (art. 261 Sr) gaat het om de 'aanranding van iemands eer of goede naam door telastlegging van een bepaald feit' 'met het kennelijke doel om daaraan ruchtbaarheid te geven' (bijvoorbeeld door middel van een beschuldiging (waaronder seksueel wangedrag (#metoo)) of een leugen (Van Noorloos, 2021). De 'eer en goede naam' kan worden omschreven als de reputatie die een persoon in het maatschappelijk verkeer geniet. Het schaden van die reputatie, iemand bij het publiek in een kwaad daglicht stellen, is dan de aanranding van de eer of de goede naam (Janssens & Nieuwenhuis, 2019). Onder 'ruchtbaarheid geven' wordt verstaan 'het ter kennis van het publiek brengen'.[105] De opzet van de dader dient dus ook op de openbaarheid te zijn gericht. Ook het plaatsen van een hyperlink op een Facebookpagina die naar

101 Hof Arnhem-Leeuwarden 20 januari 2023, ECLI:NL:GHARL:2023:528.
102 Rb. Amsterdam 17 februari 2023, ECLI:NL:RBAMS:2023:1438.
103 Zie ook Hof Den Bosch 12 oktober 2009, ECLI:NL:GHSHE:2009:BK5777.
104 HR 22 april 2014, ECLI:NL:HR:2014:952.
105 Zie bijvoorbeeld HR 8 juli 2008, ECLI:NL:HR:2008:BC9186 en HR 13 december 2016, ECLI:NL:HR:2016:2848, r.o. 2.5.1.

een beledigende tekst verwijst, kan de 'verspreiding van een geschrift en/of afbeelding' als bedoeld in artikel 261 Sr opleveren.[106] Een beschuldiging in besloten kring levert geen smaad op. Wanneer smaad plaatsvindt met een geschrift (bijvoorbeeld met een tekst of met afbeeldingen, hetgeen meestal het geval is in een digitale context), dan bedraagt de maximale gevangenisstraf één jaar.[107]

Artikel 262 Sr stelt het delict laster strafbaar. Laster verschilt van smaad in de zin dat de dader zijn beledigende bewering doet, terwijl hij weet dat deze onwaar is. Het wordt als een zwaarder delict gezien met maximale gevangenisstraf van twee jaar. In de praktijk komt vervolging van laster zelden voor, omdat de bewijslast van de wetenschap dat de beschuldiging onwaar is, erg lastig is (Janssens & Nieuwenhuis, 2019).

Eenvoudige belediging

Het delict eenvoudige belediging (art. 266 Sr) betreft 'elke opzettelijke belediging die niet het karakter van smaad heeft'. De uiting plaatst iemand in een ongunstig daglicht en randt daarmee iemands eer of goede naam aan.[108] Het uitschelden van een politieambtenaar met termen als 'imbecielen' of 'mongolen' in de openbaarheid kan bijvoorbeeld eenvoudige belediging opleveren.[109] Het verschil met de andere uitingsdelicten is dat belediging niet per se in het openbaar hoeft plaats te vinden: het kan ook rechtstreeks naar het slachtoffer zonder dat anderen erbij zijn. Op het delict eenvoudige belediging staat een maximale gevangenisstraf van drie maanden.

106 HR 18 maart 2018, ECLI:NL:HR:2018:331.

107 De maximale gevangenisstraffen voor strafbare belediging kunnen met een derde worden verhoogd als sprake is van de situatie in art. 267 Sr. In dat geval is het géén klachtdelict (art. 269 lid 2 Sr). Deze bepaling wordt verder niet besproken in dit hoofdstuk.

108 HR 30 oktober 2001, ECLI:HR:2001:AB3143 en HR 29 maart 2016, ECLI:NL:HR:2016:510.

109 Hof Leeuwarden 27 oktober 2009, ECLI:NL:GHLEE:2009:BK1484; HR 10 februari 2015, ECLI:NL:HR:2015:274 (*mierenneuker*). Het gebruik van het woord "mierenneuker" is op zichzelf niet beledigend, maar kan dit wel zijn door de context waarin dat woord is gebezigd.

Casus: belediging van Sylvana Simons

In 2016 stelde politica Sylvana Simons zich kandidaat voor de politieke partij DENK in de Tweede kamer.[110] Zij kreeg daarop met name op Facebook een stortvloed aan beledigende uitingen over zich heen voornamelijk gericht op haar huidskleur. Na aangifte van de politica werden twintig personen veroordeeld voor, onder meer, belediging.

De rechtbank Amsterdam overweegt in deze specifieke zaak dat een op Facebook geplaatst bericht moet worden aangemerkt als een geschrift. De verdachte heeft op Facebook en dus in het openbaar, het bericht geplaatst en gedeeld. Naar het oordeel van de rechtbank is deze uitlating op zichzelf geschikt om te beledigen, gelet op de verschillende daarin gebruikte scheldwoorden. Daar komt nog een racistisch element bij omdat verdachte het woord 'zwarte' gebruikt om aangeefster aan te duiden. De verdachte werd veroordeeld voor het delict 'eenvoudige belediging' en kreeg een geldboete van 150 euro opgelegd.

Discriminatie en groepsbelediging

De artikelen 137c-137e Sr bevatten strafbepalingen gericht tegen discriminerende uitlatingen. Overheden trachten bepaalde uitingen ook tegen te gaan en strafbaar te stellen om de openbare orde te handhaven, omdat uitingen tot agressie of geweld kunnen leiden, om de reputatie van personen te beschermen en om de gelijke menselijke waardigheid van groepen personen beschermen. De bepalingen over discriminatie, groepsbelediging en opruiing zijn daarom geplaatst in de titel van misdrijven tegen de openbare orde in het Wetboek van Strafrecht. De wetgever wilde voorkomen dat het publieke debat zou ontaarden in het uitschelden van bevolkingsgroepen of ongeregeldheden (Janssen & Nieuwenhuis, 2019). Daarnaast is de ratio dat het beledigen van groepen hun maatschappelijk functioneren onder druk kan zetten. De wortels van de strafbaarstelling van groepsbelediging liggen bijvoorbeeld in de jaren dertig, toen met de groei van fascisme en antisemitisme het verbod op groepsbelediging werd ingevoerd om negatieve beeldvormen over groepen te voorkomen (Van Noorloos, 2012). De uitbreiding van deze artikelen is voornamelijk ingegeven om te voldoen aan internationale verdragen en om sociale redenen, zoals de bescherming van het onbelemmerd maatschappelijk

110 H. Bahara, 'Rechtbank hoopt op "afschrikwekkend effect" met veroordeling bedreigers Sylvana Simons', *Volkskrant.nl*, 18 mei 2017.

functioneren van groepen en tot bescherming van individuele personen om zich volwaardig burger te voelen en gevrijwaard te blijven van discriminatoire uitingen (De Ruiter & Velleman, 2023).[111]

Artikel 137c Sr verbiedt de belediging op grond van de in de wet aangeduide groepskenmerken (ras, godsdienst, levensovertuiging, seksuele gerichtheid of lichamelijke, psychische of verstandelijke handicap en geslacht (Noorloos & Verrest, 2021). De verdachte moet ook (voorwaardelijk) opzet hebben gehad op de openbaarheid van de belediging.[112] Dat betekent dat de verdachte ten minste bewust de aanmerkelijke kans moet hebben aanvaard dat zijn uiting ter kennis van publiek zou komen. Op het delict staat een maximale gevangenisstraf van één jaar (en bij het maken van een beroep of gewoonte ervan maximaal twee jaar).

Kortgezegd stelt artikel 137d Sr strafbaar het aanzetten tot haat, tot discriminatie en tot gewelddadigheden wegens de bovengenoemde groepskenmerken. Op dit delict staat maximaal twee jaar gevangenisstraf of een geldboete. Ten slotte stelt artikel 137e Sr de verspreiding van deze gedragingen strafbaar. Hier staat een gevangenisstraf op van maximaal zes maanden (bij het maken van een beroep of gewoonte ervan maximaal één jaar gevangenisstraf).

Opruiing

Opruien is het aanzetten tot een strafbaar feit of tot gewelddadig optreden tegen het openbaar gezag (art. 131 Sr). De verspreiding is strafbaar gesteld in artikel 132 Sr. Hier was bijvoorbeeld sprake van in een zaak waarbij een verdachte via zijn Snapchataccount (met 10.000 volgers) een bedreiging jegens de politie uitte. Daarbij is de context belangrijk tegen de achtergrond van de gewelddadige rellen die enkele weken eerder op Urk hadden plaatsgevonden terwijl de verdachte opriep om de adressen van de agenten, die onder andere als 'kankerflikkers' werden bestempeld, te laten publiceren en mensen opriep om 'het politiebureau te laten trillen', waarbij 'mietjes' niet welkom waren.[113]

Het is niet vereist dat het strafbare feit of het geweld zich daadwerkelijk materialiseert; het gaat om het *gevaar* dat een en ander zal kunnen plaatsvinden. Het kan ook gaan om degene die met zijn uitlating willens en wetens de aanmerkelijke kans heeft aanvaard dat zijn uitlating derden zou kunnen bewegen tot het plegen van strafbare feiten (voorwaardelijk opzet)

111 Zie ook art. 1.1 van de Aanwijzing discriminatie, 2018A009.

112 HR 29 mei 2001, ECLI:NL:HR:2001:AB1818.

113 Rb. Midden-Nederland 5 januari 2021, ECLI:NL:RBMNE:2021:12.

(Janssens & Nieuwenhuis, 2019).[114] Op het delict staat – in vergelijking met de andere delicten – een relatief zware gevangenisstraf van maximaal vijf jaar of geldboete.

Casus: The Base

'The Base' betreft een terroristische organisatie, omdat het een internationaal netwerk is van rechtsextremisten die tot doel had terroristische misdrijven te plegen, zoals het begaan van doodslag met een terroristisch oogmerk (art. 288a Sr). In deze zaak beschrijft de rechtbank dat 'The Base' zichzelf ziet als een verzetsgroep tegen een door Joden gedomineerd politiek systeem. The Base verspreidt online informatie over survivaltechnieken en zelfverdediging en organiseert trainingen en ontmoetingen.

In de Telegramgroep 'Jeugdstorm', 'J.S.N.', 'Beau Sneactha' werden extreme berichten door aanhangers van The Base geplaatst.[115] De verdediging stelt dat ten aanzien van de Telegramgroep Jeugdstorm en de WhatsAppgroep de verdachte dient te worden vrijgesproken, omdat het gaat om chatverkeer binnen een besloten groep, zodat niet is voldaan aan het vereiste van openbaarheid. Volgens de rechtbank blijkt uit onderzoek van de politie dat de Telegramgroep Bua Sneachta openbaar is. Hoewel de Telegramgroepen Jeugdstorm en J.S.N. slechts respectievelijk 21 en 30 deelnemers hadden, was de rechtbank van oordeel dat de groepen op zichzelf een publiek vormen en de uitlatingen binnen de groep in de openbaarheid zijn gebracht.

De rechtbank acht verder de meeste ten laste gelegde uitlatingen in de Telegramgroep Bua Sneachta 14/88, 'zonder meer' opruiend van aard, aangezien wordt opgeroepen tot geweld c.q. het doden van gekleurde mensen, homoseksuelen en Joden. In de Telegramgroep Jeugdstorm heeft de verdachte verder opgeruid tot het doden dan wel ontvoeren van een willekeurig persoon en het jagen op pedoseksuelen. Ook heeft de verdachte een andere deelnemer aangemoedigd in zijn wens om een soortgelijke aanslag te plegen zoals Brenton Tarrant op twee moskeeën

114 Zie bijvoorbeeld HR 29 mei 2001, ECLI:NL:HR:2001:AB1818.

115 Zie over de zaak ook C. Rosman, 'Nederlandse aanhangers "rassenoorlog" hoeven niet terug de cel in', *Het Parool*, 2 december 2021.

in Christchurch (Nieuw-Zeeland) heeft gedaan, waarbij 51 mensen om het leven kwamen. De verdachte oppert in dit verband een synagoge. Een aanslag op een (Joods) gebedshuis is volgens de rechtbank ontegenzeggelijk opruiing tot een terroristisch misdrijf (art. 131 lid 2 Sr). In de WhatsAppgroep J.S.N heeft de verdachte volgens de rechtbank opgeruid, omdat werd opgeroepen 'tot het ontvoeren van een neger die in een bos wordt gedropt zodat op hem kan worden gejaagd', hetgeen past in de ideologie van het rechtsextreme accelerationisme, en daarmee als een terroristisch misdrijf kan worden beschouwd. Vanuit diezelfde ideologie heeft de verdachte opgeruid tot het doden van blanken die niet 'aan hun kant' staan en niet willen veranderen, hetgeen eveneens opruiing tot een terroristisch misdrijf oplevert. Daar waar de rechtbank opruiing bewezen acht, komt zij tevens tot bewezenverklaring van verspreiding (art. 132 Sr), vanwege het delen van een afbeelding waarop een knielende Joodse man door zijn hoofd wordt geschoten.

De verdachte is in deze zaak veroordeeld tot een gevangenisstraf van twee jaar, waarvan achttien maanden voorwaardelijk, een taakstraf van tweehonderd uur en een proeftijd van drie jaar. De rechtbank verbindt daaraan opvallend bijzondere voorwaarden. Zo mag de veroordeelde: 'zich niet online bevinden op de verborgen websites van Dark Web en (...) geen software gebruiken om anonimiteit te verschaffen zoals Tor, I2P of Freenet'. Daarnaast 'moet hij meewerken aan controle van zijn digitale gegevensdragers tijdens een huisbezoek'.[116]

Bedreiging

Bedreiging met het 'openlijk geweld plegen tegen personen of goederen', 'met enig misdrijf waardoor gevaar voor de algemene veiligheid van personen of goederen of gemeen gevaar voor de verlening van diensten ontstaat', of 'met verkrachting, met feitelijke aanranding van de eerbaarheid, met enig misdrijf tegen het leven gericht, met gijzeling, met zware mishandeling of met brandstichting', is strafbaar gesteld in artikel 285 Sr, met een maximale gevangenisstraf van twee jaar of een geldboete.[117] Volgens de rechtspraak van artikel 285 Sr moet strafbare bedreiging verder de kernelementen vrees en opzet bevatten en geloofwaardig zijn: de bedreiging moet ter kennis van de bedreigde zijn gekomen en de bedreiging moet van een zodanige aard zijn en

116 Rb. Rotterdam 2 december 2021, ECLI:NL:RBROT:2021:11858.

117 In lid 2, 3 en 4 staan strafverzwarende omstandigheden.

onder zodanige omstandigheden zijn geschied dat bij bedreigde een redelijke vrees heeft kunnen ontstaan dat de bedreiging ook daadwerkelijk ten uitvoer zal worden gelegd (De Haan & Nijboer, 2007).

Ook hier is het afhankelijk van de omstandigheden van het geval of sprake is van bedreiging. De toevoeging 'Doe de groeten aan uw dochter... en uhm, zorg ervoor dat ze in de gaten wordt gehouden' in een e-mail aan de fractievoorzitter van een politieke partij, kan bijvoorbeeld een strafbare bedreiging opleveren.[118] Ook een poging tot bedreiging is mogelijk. Zo is een dader al eens veroordeeld omdat hij op Facebook met een openbaar profiel met 158 vrienden een bedreiging uitte naar voormalig koningin Beatrix en premier Rutte door te stellen dat zij dood moesten en daarbij te refereren naar *high school shooters* en bekende moordenaars.[119]

Doxing

In 2023 is het delict doxing strafbaar gesteld in artikel 285c Sr. Het artikel stelt strafbaar 'degene die zich persoonsgegevens van een ander of een derde verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk om die ander vrees aan te jagen, enige overlast aan te doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen'. De wetgever heeft het delict ook wel omschreven als het openbaar maken van iemands persoonlijke, sensitieve en privé-informatie zoals adres, telefoonnummer, paspoort, werkgever, gegevens van familie en foto's van de kinderen.[120] Op het delict staat een maximale gevangenisstraf van een jaar of een geldboete van de derde categorie.

Voor strafbare doxing is niet vereist dat het slachtoffer wordt bedreigd met een bepaald ernstig misdrijf. Het OM zal doorgaans een strafrechtelijk onderzoek starten na een melding of aangifte van het slachtoffer, maar een klacht van het slachtoffer is niet vereist (het is dus geen klachtdelict).

De strafbaarstelling van doxing werd noodzakelijk geacht, omdat de impact op de slachtoffers en naasten groot kan zijn. Zo werden bijvoorbeeld uit onvrede met het vaccinatiebeleid tijdens de coronacrisis in Telegramgroepen rondom de 'avondklokrellen' lijsten met namen en adresgegevens geopenbaard van leden van de Tweede Kamer en van medewerkers van het RIVM en van de GGD die werkzaam waren op priklocaties. In chatgroepen werden

118 HR 7 juli 2015, ECLI:NL:HR:2015:1790.
119 Hof Den Bosch 16 mei 2014, ECLI:NL:GHSHE:2014:1393.
120 *Kamerstukken II* 2021/22, 36171, nr. 3, p. 1.

oproepen gedaan om persoonsgegevens zoals een woonadres te achterhalen van overheidsfunctionarissen, journalisten en wetenschappers, bestuurders en politici, of van medewerkers van bepaalde bedrijven. Deze gegevens werden vervolgens via sociale media verder verspreid, veelal gecombineerd met het plaatsen van een herkenbare foto, en een oproep om de betrokkene thuis een bezoek te brengen. Ook politieagenten, opiniemakers, journalisten en politici hebben volgens de wetgever in toenemende mate te maken gekregen met online intimidatie en bedreiging.[121]

Wij merken nog wel op dat de wetgever erkent dat het vergaren, het samenbrengen en het publiceren van persoonsgegevens ook een gerechtvaardigd belang kan dienen. Hij noemt expliciet in de memorie van toelichting dat dit bijvoorbeeld het geval is wanneer de intentie bij het verzamelen en publiceren van persoonsgegevens is gericht op nieuwsgaring of op het aan de kaak stellen van misstanden. Bij journalistieke uitingen zal er geen sprake zijn van een oogmerk in de zin van artikel 285d, zodat er geen strafbare gedraging is en geen vervolging zal worden ingesteld.[122] Het is bovendien in het geval van doxing de bedoeling dat 'eerst en vooral' moet worden ingezet op andere (preventieve) maatregelen, zoals het bevorderen van een veilige online omgeving, bewustwording, het via de (internet) host van het medium weghalen van de gegevens op basis van de Gedragscode Notice-and-Take-Down of een civiele procedure (zie hieronder) Dit moet het OM in zijn vervolgingsbeleid meenemen (Nan & Schemer, 2023).

4.7.3 Het verwijderen van strafbaar materiaal

Wanneer een burger aangifte doet van strafbare content op het internet, staat voor het Openbaar Ministerie de bevoegdheid van artikel 126p Sv open. Deze bevoegdheid wordt ook wel het 'ontoegankelijkheidsmakingsbevel' of 'take down-bevel' genoemd (Oerlemans, 2017b). De achtergrond van deze regeling is gelegen in het uitgangspunt dat internetaanbieders als 'doorgeefluik' fungeren en niet aansprakelijk zijn voor het gedrag van gebruikers over hun netwerken. Pas na een rechterlijk bevel zijn zij verplicht gegevens te verwijderen.[123] In artikel 54a Sr staat ook expliciet dat een tussenpersoon

121 *Kamerstukken II* 2021/22, 36171, nr. 3, p. 2.

122 *Kamerstukken II* 2021/22, 36171, nr. 3, p. 9.

123 Internetdienstverleners kunnen ook verplicht worden gegevens te verwijderen met civiele instrumenten. Ook zal in Nederland de 'Autoriteit Online Terroristisch en Kinderpornografisch Materiaal' via het bestuursrecht de verwijdering van materiaal kunnen afdwingen. Ten slotte brengt de Digitalemarktenverordening (de Digital Ser-

die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens niet wordt vervolgd bij een strafbaar feit dat met gebruikmaking van die dienst door een ander wordt begaan, indien hij voldoet aan een bevel als bedoeld in artikel 125p Sv.[124]

De officier van justitie kan, na een machtiging van een rechter-commissaris, het ontoegankelijkheidsmakingsbevel van artikel 126p Sv aan de aanbieder van een communicatiedienst sturen en eisen dat terstond alle maatregelen worden genomen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken. Het bevel kan alleen worden gegeven in geval van verdenking van misdrijven waarvoor voorlopige hechtenis mogelijk is (art. 67 Sv). Bij uitingsdelicten gaat het dan bijvoorbeeld om opruiing en overige delicten genoemd in artikel 67 lid 1 sub b Sv.

Het idee is dat het bevel pas wordt gegeven, als de aanbieder geen opvolging heeft gegeven aan een verzoek tot *notice and take down*.[125] Ook kan de politie of het OM een verzoek doen tot verwijdering of ontoegankelijkheidsmaking, waaraan de internetdienstverlener vrijwillig kan voldoen. Als de inzet van de bevoegdheid toch noodzakelijk is en niet wordt voldaan aan het ontoegankelijkheidsmakingsbevel, kan vervolging worden ingesteld voor het niet voldoen aan een bevoegd gegeven ambtelijk bevel (art. 184 Sr) en onder omstandigheden voor het deelnemen of medeplegen aan het gronddelict.[126] Als de officier van justitie en de betrokkene het niet met elkaar eens zijn, staat de beklagregeling in artikel 552a Sv open.

Of het materiaal na een melding in de praktijk daadwerkelijk wordt verwijderd is afhankelijk van verschillende factoren. Het is bijvoorbeeld technisch niet altijd mogelijk gegevens te verwijderen. Ook kan de relatie met de betreffende dienstverlener zeer slecht zijn of zich in een jurisdictie bevinden waar andere regels gelden (Van Hoboken et al., 2020). Het Nederlandse kabinet wijst er bijvoorbeeld op dat de relatie Telegram en de Nederlandse politie zeer slecht is. Dat maakt het lastig om Telegramkanalen te blokkeren en

vice Act) nieuwe verplichtingen met zich mee over het verwijderen onrechtmatige en illegale content.

124 Of een beslissing als bedoeld in art. 3 lid 1 Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud (*PbEU* 2021, L 172).

125 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 57.

126 *Kamerstukken II* 2016/17, 34372, nr. 6, p. 109.

gebruikers te achterhalen.[127] Politiediensten wijzen ook op het bestaan van *bullet proof hosting* providers die vanwege hun verdienmodel niet, zo laat als mogelijk (of pas na het informeren van klanten), materiaal verwijderen van hun servers (Europol, 2023b).

Het idee is dat proportioneel wordt gehandeld bij de inzet van een *take down*-bevel. Dat betekent dat de bevoegdheid stapsgewijs moet worden ingezet. Eerst moet de plaatser van het onrechtmatige materiaal worden aangesproken het materiaal te verwijderen. Als deze niet aan het bevel voldoet of aanspreekbaar is, kunnen de autoriteiten naar de websitehouders stappen. Als deze ook niet voldoet of aanspreekbaar is, kunnen de autoriteiten naar een hosting provider stappen. Als deze ook niet voldoet of aanspreekbaar is, is zelfs denkbaar dat aan de internet access provider een ontoegankelijkheidsmakingsbevel wordt opgelegd. In dat geval wordt een website ontoegankelijk gemaakt door middel van een internetfilter. In Nederland zijn vooralsnog alleen in civielrechtelijke procedures Vodafone/Ziggo en KPN verplicht 'The Pirate Bay' te blokkeren, vanwege schending van auteursrechten.[128]

Bij elke stap moet worden afgewogen of het doel (de ontoegankelijkheidsmaking) nog wel opweegt tegen de inbreuk op fundamentele rechten (met name de toegang tot informatie als onderdeel van de vrijheid van meningsuiting) (Kuş & Ten Voorde, 2014). Daarbij moet er ook aandacht zijn in hoeverre te veel informatie ontoegankelijk wordt gemaakt. Tot nog toe is er weinig jurisprudentie beschikbaar over het ontoegankelijkheidsmakingsbevel.

4.8 Toekomstige ontwikkelingen

In deze laatste paragraaf bespreken we twee toekomstige ontwikkelingen die naar alle waarschijnlijkheid een rol gaan spelen in de toekomst bij gedigitaliseerde criminaliteit, namelijk het toenemende gebruik van AI en criminaliteit in 'virtual reality'.

127 Antwoord op vragen van de Kamerleden Kuik en Slootweg over het bericht 'Telegram treedt niet effectief op tegen op grote schaal delen van contactgegevens en naaktfoto's van vrouwen' van 11 oktober 2023, *Handelingen II* 2023/24, 212.

128 HR 29 juni 2018, ECLI:NL:HR:2018:1046 en Hof Amsterdam 2 juni 2020, ECLI:NL:GHAMS:2020:1421.

4.8.1 AI en gedigitaliseerde criminaliteit

Het toenemende gebruik van AI is al diverse malen in dit boek aan bod gekomen. Zo kwam in hoofdstuk 2 en 3 al naar voren dat AI in toenemende mate een rol kan spelen bij het ontwikkelingen van malware en het ondetecteerbaar maken ervan. De verwachting is ook dat cybercriminelen *Large Language Models* (LLM's), zoals ChatGPT, gebruiken om zeer geloofwaardige phishingmails of conversaties met slachtoffers te houden om daarmee oplichting te plegen.

Europol (2023a) wijst ook op de mogelijkheden van AI voor het maken van deepfakes en andere synthetische media (zoals audiofakes). Zoals al eerder in dit hoofdstuk is opgemerkt zijn bekende (vaak vrouwelijke) personen al eens slachtoffer geworden van seksuele deepfakes of audiofakes. Wetenschappers waarschuwen ook voor andere gevaren van deepfakes, zoals voor het gebruik bij het maken van desinformatie tijdens verkiezingen (Van der Sloot et al., 2021). Uitingsdelicten, zoal smaad, discriminatie en opruiing, kunnen ook grootschaliger en geautomatiseerd plaatsvinden met behulp van AI.

Ten slotte wijst Europol (2023a) ook op de opkomst van *dark LLM's*, die op het dark web worden gehost en een chatbot leveren zonder enige beveiliging, alsmede LLM's die worden getraind op bepaalde – wellicht bijzonder schadelijke – gegevens, zoals seksueel materiaal van minderjarigen. Opsporingsinstanties zullen zich hierop moeten voorbereiden, onder andere door bewustwording en het ontwikkelen van vaardigheden om zelf deze technologie voor de eigen taakuitvoering te gebruiken.

4.8.2 Criminaliteit in virtual reality- en mixed reality werelden

Een hele andere ontwikkeling die in de toekomst gaat spelen in het cyberdomein is het belang van *augmented* en *virutal reality*. Bij augmented reality wordt onze perceptie van de wereld uitgebreid doordat virtuele elementen worden toegevoegd aan de realiteit, bijvoorbeeld door middel van apparaten zoals smartphones, augumented reality-brillen of games zoals Pokémon Go. Bij virtual reality wordt de fysieke wereld zo veel mogelijk vervangen door een kunstmatige of virtuele werkelijkheid, bijvoorbeeld door een virtual reality-bril. Uit onderzoek komt naar voren dat het huidige juridische kader in algemene zin goed is toegerust om de mogelijke negatieve effecten van immersieve technologie te adresseren (Schermer & Van Ham, 2021).

Het kabinet vond het in 2023 'zeer zorgwekkend' dat in het onderzoek van Schermer & Van Ham (2021) is vastgesteld dat slachtoffers van virtuele aanranding een vergelijkbare emotie ervaren als bij een fysieke aanranding of verkrachting, en dat de onderzoekers verwachten dat naarmate de immersie en het gevoel van aanwezigheid in een virtuele omgeving groter wordt, de impact van virtueel grensoverschrijdend gedrag ook groter kan worden.[129] Deze technologieën zorgen voor nieuwe vragen, bijvoorbeeld of virtuele mishandeling of virtueel vandalisme beter strafbaar moeten worden gesteld (Strikwerda, 2014; Ten Voorde, 2017b).[130]

4.9 Tot besluit

In dit hoofdstuk zijn de belangrijkste verschijningsvormen van gedigitaliseerde criminaliteit uitgelegd. U begrijpt op welke wijze deze misdrijven doorgaans worden gepleegd en op welke manier zij strafbaar zijn gesteld. Zoals we hebben gezien, zijn in de praktijk vaak verschillende delicten tegelijk van toepassing, met soms een combinatie van cybercriminaliteit in enge zin of traditionele criminaliteit. Het is bijvoorbeeld mogelijk om oplichting te plegen nadat de financiële persoonsgegevens zijn overgenomen door computervredebreuk en het installeren van malware. Vaak werken de betrokkenen samen in een crimineel samenwerkingsverband. Het verdiende geld kan vervolgens worden witgewassen via bitcoins. Het illustreert ook de realiteit van 'hybride' (cyber)criminele netwerken (zie verder hoofdstuk 6).

Ook hebben we gezien dat de strafbaarstelling van veel delicten, in het bijzonder als het gaat om uitingsdelicten, niet altijd eenvoudig is te beantwoorden. De vraag of een uiting strafbaar is, moet aan de hand van een concrete situatie worden beantwoord. Bovendien kunnen het algemeen belang en de vrijheid van meningsuiting prevaleren boven de vermeende strafbaarheid van de uiting en is het strafrecht niet altijd het beste middel om schadelijke uitingen te bestrijden.

129 Beleidsreactie op de WODC-onderzoeken naar de regulering van deepfakes en immersieve technologieën, 16 juni 2023.

130 Elisa Heisen, 'Aanranding bestaat ook in virtual reality: "Lijkt echt met zo'n bril op"', *Nu.nl*, 21 februari 2022.

4.10 Discussievragen

1. Is het onderscheid tussen cybercriminaliteit in enge zin en gedigitaliseerde criminaliteit wel altijd scherp?
2. Bij welke delicten is er duidelijk sprake van vervlechting van de offline en online wereld?
3. Wat vindt u na het lezen van dit hoofdstuk van de stelling: 'De wet loopt altijd achter bij de technologische ontwikkelingen'?
4. Is het wenselijk het fenomeen 'seks-chatten' strafbaar te stellen?
5. Wat vindt u van het feit dat virtuele kinderpornografie strafbaar is gesteld?
6. Bent u het met de overheid eens dat cryptogeld geen 'echt' geld is?
7. Zijn seksuele deepfakes voldoende strafbaar gesteld?
8. Doet het Wetboek van Strafrecht voldoende recht aan mogelijk leed dat wordt ervaren in de virtuele wereld?
9. Zou verkrachting in een virtuele wereld strafbaar moeten zijn?
10. Vindt u het terecht dat veel uitingsdelicten zogenoemde 'klachtdelicten' zijn?
11. Worden uitingsdelicten in dit boek terecht aangemerkt als gedigitaliseerde criminaliteit?
12. Is het strafrecht het beste middel om uitingsdelicten tegen te gaan?

4.11 Kernbegrippen

- Belediging
- Bitcoin
- Botnet
- Computervredebreuk
- Dark web
- Darknetmarkt
- Ddos-aanval
- Doxing
- Ethisch hacken
- Grooming
- Hacking
- Hate speech
- Internetoplichting
- Identiteitsfraude
- Malware

- Marktplaatsoplichting
- Materiaal van seksueel misbruik van minderjarigen
- Notice-and-Takedown
- Online handelsplaats
- Ontoegankelijkheidsmaking
- Opruiing
- Phishing
- Ransomware
- Sekschatten
- Sexting
- Sextortion
- Smaad
- Tor
- Uitingsdelicten
- (Virtuele) kinderpornografie
- Witwassen (online)
- Wraakporno