REDACTIONEEL

Ongewenst gedrag online

Marleen Weulen Kranenbarg, Robby Roks & Lisa van Reemst

Sinds het ontstaan van het internet in de jaren zeventig van de vorige eeuw is er in de criminologie aandacht voor wat deze digitale revolutie betekent voor criminaliteit en de bestrijding hiervan. Veel wetenschappelijke aandacht is hierbij de afgelopen jaren uitgegaan naar cybercriminaliteit. Dit redactioneel van het themanummer over ongewenst gedrag online kan gezien worden als uitnodiging voor de Nederlandse criminologie om zich breder te verhouden tot de digitalisering van onze samenleving. Ongewenst gedrag online, zo maken de bijdrages in dit themanummer duidelijk, kent bijzonder uiteenlopende verschijningsvormen. Wat deze bijdrages verbindt, zijn de criminologisch relevante vragen rondom de strafbaarheid, maar ook de schadelijkheid van het gedrag en in het bijzonder of dit nu betrekking heeft op de online content of de offline gevolgen hiervan. Hierbij rijst eveneens de vraag of het denken in een dergelijke binaire oppositie wel voldoende recht doet aan de complexe wisselwerking en intense verwevenheid tussen het online en offline domein. Ten slotte illustreren de bijdrages in dit themanummer eveneens dat de digitalisering heeft geresulteerd in de nodige digitale artefacten om te onderzoeken.

Inleiding

Het internet is niet meer weg te denken uit het leven van de meeste Nederlanders, zo valt te lezen in de webpublicatie 'ICT, kennis en economie' van het Centraal Bureau voor de Statistiek (CBS, 2023). In 2022 had 97 procent van de Nederlanders van 12 jaar en ouder thuis toegang tot internet en waren bijna negen op de tien Nederlanders (vrijwel) dagelijks online. Deze cijfers maken duidelijk dat toegang tot het internet verworden is tot een vanzelfsprekendheid: mensen *gaan* niet langer online voor informatie, vermaak of nieuwsgaring, maar ze *zijn* online (vgl. Negroponte, 1995, p. 6; Lupton, 2014, p. 168).[1] Alhoewel in deze context vooral wordt gewezen op zogenoemde 'digital natives' (zie o.a. boyd, 2014, pp. 177-180) als gen Z'ers, wordt ook bij andere generaties duidelijk hoezeer zij dagelijks afhankelijk zijn van een stabiele internetverbinding.

Ondanks deze ontwikkelingen lijkt ons denken en spreken over digitale technologie nog veelal te rusten op dichotomieën als online versus offline en digitaal versus fysiek, bijvoorbeeld wanneer we het hebben over online versus offline communicatie. Powell et al. (2018, p. 7) menen dat een dergelijk onderscheid ten tijde van de opkomst van online vormen van communicatie en virtuele gemeenschappen in de jaren negentig van de vorig eeuw nog viel te billijken, maar dat dit tegenwoordig

1 Met dank aan Jeroen van den Broek voor deze verwijzing.

niet langer recht doet aan de verwevenheid van digitale technologieën met allerhande facetten van het dagelijks leven. Het zal de kritische lezer niet zijn ontgaan dat de titel van dit themanummer ook lijkt te vertrekken vanuit de binaire oppositie tussen online en offline vormen van ongewenst gedrag. We zullen de keuze voor deze focus en titel in de loop van dit redactioneel toelichten. Daarvoor beginnen we met het bespreken van wat door verschillende auteurs is aangeduid als de digitale criminologie. Vervolgens gaan we nader in op het bestuderen van ongewenst gedrag online. We besluiten deze bijdrage met het geven van een beeld van de artikelen in dit themanummer, met bijzondere aandacht voor wat deze bijdrages inhoudelijk alsook methodologisch met elkaar verbindt.

Naar een digitale criminologie?

Sinds het ontstaan van het internet in de jaren zeventig van de vorige eeuw is er aandacht voor wat deze digitale revolutie betekent voor criminaliteit en de bestrijding hiervan, waarin de focus vooral lag op cybercriminaliteit (Van der Wagen et al., 2024, pp. 23-36). Cybercriminaliteit kan hierdoor beschouwd worden als een relatief jong aandachtsgebied in de criminologie. Inmiddels elf jaar geleden formuleerden Van Erp et al. (2013) in het vorige themanummer over dit onderwerp in het *Tijdschrift voor Criminologie* dan ook de nodige empirische, theoretische en methodologische vragen voor de bestudering van criminaliteit in de gedigitaliseerde samenleving. Een flink deel van deze vragen is inmiddels onderwerp van studie in een snelgroeiend onderzoeksveld (zie o.a. Holt, 2023; Weulen Kranenbarg & Van 't Hoff-de Goede, 2023; Van der Wagen et al., 2024).

Inmiddels lijkt de term 'cyber' ingebed te zijn in het criminologisch taalgebruik. Toch is het de vraag of dit bekende voorvoegsel volledig de lading dekt van fenomenen die worden getypeerd als 'cyber' (zie o.a. Stratton et al., 2017; Powell et al., 2018). Diverse auteurs betogen namelijk dat het gebruik van de term 'cyber' lijkt te impliceren dat het gaat om criminologische fenomenen die volledig digitaal, virtueel of online zijn (zie o.a. Brown, 2006; Hayward, 2012; Stratton et al., 2017; Graham et al., 2024). Het gebruik van de term impliceert immers een dualisme waarbij cybercriminaliteit veelal wordt beschouwd 'as a mirror or the online double of their terrestrial counterparts, differing perhaps by medium and reach, but not by nature' (Stratton et al., 2017, p. 22). Te denken valt bijvoorbeeld aan cyberpesten en cyberstalking als volledig online equivalenten van verschijningsvormen die lange tijd beperkt bleven tot de fysieke wereld. Deze varianten van cybercrime worden ook wel gedigitaliseerde criminaliteit genoemd, waarbij ICT (in dit geval online communicatiemiddelen) een middel is, maar niet het doel (in dit geval de persoon die gepest of gestalkt wordt). Dit als tegenhanger van cybercriminaliteit in enge zin, waarbij ICT zowel het middel als het doel is, zoals het hacken (digitaal middel) van ICT-systemen (digitaal doel).

Voordat de term 'cyber' in het criminologische landschap in zwang raakte, merkte Brown (2006, p. 236) al op dat 'there is quite simply no such thing as a "technological" crime (such as a "cybercrime") as distinct from an "embodied" crime'. Sterker nog, Brown (2006, p. 224) betoogt dat dit binaire denken in de criminologie de

doi: 10.5553/TvC/0165182X2024066003001

discipline belemmert in de analyse van de complexe, technosociale kenmerken van criminologische fenomenen. Met 'technosociaal' wordt in deze context gewezen op de verwevenheid tussen technologie en de mens. Brown (2006) pleit om die reden ook voor een 'criminology of hybrids' (zie o.a. Van der Wagen, 2018). Recentelijk stelde Di Nicola (2022) op een vergelijkbare wijze dat er behoefte is aan een theoretische benadering in de criminologie die verder gaat dan het dichotome onderscheid tussen on- en offline en recht doet aan de grote veranderingen in de digitale samenleving. In de context van georganiseerde criminaliteit wijst de auteur hierbij onder andere op:

> '(...) groups of individuals (and of individuals and machines, of actants) working together with different forms of specialization and professionalism and organizing in different ways to commit criminal activities online, offline/online, and offline that require organization of criminal work over a long, extended period of time and that are strongly influenced by the digital dimension in terms of the criminal activities they commit and the way these activities are organized, the organization of the criminal group itself, and the relationships with other criminal groups and criminal actors and machines'. (Di Nicola, 2022, p. 13)

De hybridisering die Di Nicola (2022) beschrijft in de context van georganiseerde criminaliteit kent hiermee verschillende aspecten en dimensies, waaronder ook relaties tussen menselijke en niet-menselijke actoren in deze (cyber)criminele vormen van samenwerking (Van der Wagen, 2018).

Voortbouwend op het werk van Brown (2006) hebben auteurs gepleit voor een digitale criminologie (Stratton et al., 2017). Een eerste vertrekpunt van deze digitale criminologie is het loslaten van de veel gehanteerde binaire opposities tussen online en offline en de fysieke en digitale wereld. In een deel van de cybercriminologische literatuur is hier nadrukkelijk aandacht voor. De nadruk op het online of digitale karakter van cybercriminaliteit gaat volgens auteurs immers voorbij aan de offline aspecten van deze delicten (Leukfeldt, 2016; Lusthaus, 2018; Lusthaus & Varese, 2021), de lokale inbedding van cybercriminele netwerken (Leukfeldt, 2016; Kruisbergen et al., 2018; Leukfeldt et al., 2019) en, meer in het algemeen, de menselijke factor van cybercriminaliteit (Leukfeldt & Weulen Kranenbarg, 2017). Een voorbeeld is een studie van Roks et al. (2021), waarin wordt gewezen op het toenemende gebruik van digitale technologie binnen de straatcultuur, resulterend in een digitalisering van traditionele straatcriminaliteit, zoals de straathandel van drugs via socialemediaplatforms, maar ook in de betrokkenheid bij phishing en andere vormen van online fraude. Leukfeldt en Roks (2021) maken in een analyse van opsporingsonderzoeken over cybercriminele netwerken op een vergelijkbare manier inzichtelijk dat de daders zich zowel bezighouden met online vormen van criminaliteit als met meer traditionele delicten, zoals de handel in verdovende middelen en gestolen goederen.

Deze voorbeelden illustreren dat de recente bestudering van cybercriminaliteit zich niet beperkt tot digitale technologie of het online domein als het gaat om het ontstaan, de organisatie of de uitvoering van criminaliteit. De digitale criminologie

gaat echter over meer dan deze vervagende grenzen tussen online en offline. In navolging van Hayward (2012) wordt door auteurs gewezen op de meer fundamentele transformatie van het dagelijks leven. Te denken valt hierbij aan de veranderende omgangsvormen en -normen tussen mensen als gevolg van ons gebruik van digitale communicatiemiddelen. De pleitbezorgers van een digitale criminologie wijzen hierbij op een breed scala aan relevante vraagstukken, waaronder de rol van technologieën in een steeds breder scala aan misdrijven, de rol van online en offline ervaringen in de strafrechtspleging, online vormen van slachtofferschap, digitale ongelijkheid, online bewegingen die strijden voor sociale rechtvaardigheid, digitale burgerwachten en Open Source Intelligence in politiewerk (Stratton et al., 2017, p. 23). Ook aandacht voor digitale surveillance kan onder de digitale criminologie geschaard worden (Schuilenburg, 2024). Aan deze lijst met onderwerpen zou wat ons betreft ook ongewenst gedrag online toegevoegd kunnen worden. We zien dit themanummer dan ook als een uitnodiging voor de Nederlandse criminologie om zich breder te verhouden tot de digitalisering van onze samenleving dan de bestudering van cybercriminaliteit, een punt dat tijdens het meest recente congres van de Nederlandse Vereniging voor Criminologie in juni 2024 door de NVC Cybercrime Divisie eerder werd gemaakt. Ook leden van de European Society of Criminology Cybercrime Working Group identificeren dit, naast preventie, als een van de belangrijkste onderwerpen om in de komende jaren meer onderzoek naar te doen, zowel op het gebied van daderschap als op het gebied van slachtofferschap (Weulen Kranenbarg & Van 't Hoff-de Goede, 2023).

Ongewenst gedrag online

Toen de themaredactie een nummer over ongewenst gedrag online wilde organiseren, vroeg zij in de call for papers expliciet om onderzoek naar zowel bestaande strafbare feiten of vormen van ongewenst gedrag die tegenwoordig ook online worden uitgevoerd, alsook ongewenste activiteiten die enkel online plaatsvinden. Voordat we een beschrijving geven van enkele overeenkomsten tussen de bijdrages die in het onderhavige themanummer zijn gepubliceerd, verdient eerst de term 'ongewenst gedrag online' nadere aandacht. Het verschijnen van dit themanummer volgt op het recent gepubliceerde *The Routledge international handbook of online deviance* (Graham et al., 2024). In de introductie van dit handboek verklaren de auteurs hun keuze voor de term online *deviantie* in plaats van online *criminaliteit*. In dit laatste geval gaat het immers om sociale constructies, oftewel om gedragingen die strafbaar zijn gesteld in een juridische bepaling, die veelal geen gelijke tred houden met technologische ontwikkelingen. Met een nadruk op online deviantie wordt een breder scala aan online gedragingen gevangen die niet per definitie strafbaar zijn, maar wel afwijken van een norm of gezien worden als sociaal onaanvaardbaar (Graham et al., 2024, p. 3).

In het onderhavige themanummer introduceren we met onze keuze voor 'ongewenst gedrag online' bewust een element van normativiteit als het gaat om online gedragingen. Hierbij kiezen we voor een engere focus dan online deviantie en een bredere focus dan online criminaliteit. Ongewenst gedrag online kan daarmee ver-

Tijdschrift voor Criminologie 2024 (66) 3
doi: 10.5553/TvC/0165182X2024066003001

wijzen naar gedragingen die zich online afspelen, maar niet per definitie strafbaar zijn. Wel gaat het over gedragingen waarbij sprake is van een zekere sociale normschending, alsook om gedrag dat gezien kan worden als schadelijk. Bij dit laatste dient echter opgemerkt te worden dat schadelijkheid, bezien vanuit een 'social harm'-benadering (Hillyard & Tombs, 2007), in een online context omgeven is met de nodige complexiteit (Lavorgna, 2021). Hierbij speelt onder andere de vraag of het online gedrag zelf gezien kan worden als schadelijk, of dat het eerder gaat over de schadelijke offline gevolgen van deze gedragingen. Ondanks dat het themanummer een focus legt op ongewenst gedrag online, blijven de bijdrages in dit themanummer, zoals we in de volgende paragraaf zullen toelichten, niet beperkt tot het online domein.

Het huidige themanummer

Wanneer we naar de bijdrages in dit themanummer kijken, dan valt op dat hier juist geen onderzoek naar vormen van cybercriminaliteit, zoals hacken of ddos-aanvallen, tussen zitten. Hoewel dit in Nederland veelvuldig onderwerp van studie is (zie o.a. Weulen Kranenbarg & Van 't Hoff-de Goede, 2023), heeft onze vraag naar artikelen over 'ongewenst online gedrag' duidelijk een bredere groep auteurs aangesproken. Op het eerste oog lijken de gepubliceerde papers in dit themanummer te gaan over sterk uiteenlopende fenomenen. Het artikel van **Hill en Weulen Kranenbarg** gaat over het verspreiden van desinformatie over het klimaat, **Van der Vegt** buigt zich over de samenhang tussen complottheorieën en online haat gericht tegen politici, **Roks, De Jong en Van den Broek** belichten het vraagstuk van authenticiteit in de Nederlandse online drillrapcultuur, **Blokland, Daser, De Boer, Gannon, Gnielka, Huikuri, Reichel, Schmidt, Staciwa en Lehmann** richten zich op communicatiepatronen op darknet-seksueelkindermisbruikforums, en **Notté, Tierolf, Meurens en Elphick** behandelen ten slotte de onveiligheid van kinderen als het gaat om de blootstelling aan digitale vormen van seksuele kinderuitbuiting. We beginnen met het benoemen van enkele thematische overeenkomsten en besluiten deze bijdrage met het schetsen van enkele gelijkenissen als het gaat om de digitale artefacten die zijn bestudeerd.

Overkoepelende bijzonderheden

Een eerste blik op de gedragingen in de verschillende artikelen maakt duidelijk dat het in lang niet alle gevallen gaat over criminaliteit. In de verschillende artikelen komt de term 'criminaliteit' dan ook nauwelijks voor, maar wordt vooral de verschijningsvorm beschreven. In het geval van het verspreiden van digitale content over seksueel kindermisbruik, zoals in de bijdrages van **Blokland et al**. en **Notté et al**., is de strafbaarstelling van het gedrag het meest duidelijk (zie o.a. Oerlemans et al., 2024, pp. 129-135). Ook het verspreiden of aanzetten tot haat via sociale media (**Van der Vegt**) is als zogenoemd online uitingsdelict strafbaar, alhoewel de vraag of een specifieke uiting strafbaar is zich in juridische zin niet altijd eenvoudig laat beantwoorden (Oerlemans et al., 2024, pp. 146-155). Iets vergelijkbaars geldt voor de communicatie van geweld in de online drillrapcultuur (**Roks et al**.): ook daar

zien we online uitingen die in sommige gevallen geclassificeerd kunnen worden als strafbare vormen van bedreiging, maar dit is niet altijd zonneklaar (Oerlemans et al., 2024, pp. 155-156).

In het geval van het verspreiden van complottheorieën (**Van der Vegt**) of desinformatie (**Hill & Weulen Kranenbarg**) is het eveneens maar zeer de vraag of we kunnen spreken van strafbaar gedrag, oftewel of het hier gaat over criminaliteit. Wel zien we in dit voorbeeld duidelijk terug hoe het internet bijdraagt aan het ontstaan van online gedragingen die we als maatschappij ongewenst vinden, in het bijzonder vanwege de mogelijke gevolgen in de fysieke wereld. Hierdoor ligt de nadruk dan ook vaak op de mogelijke maatschappelijke schade van het gedrag in het algemeen en niet op de specifieke gevolgen van één specifieke gedraging (het schadebeginsel, zie o.a. Bisschop, 2021; Hillyard & Tombs, 2007; Lynch, 1990; Mooney, 2020). Soms is die schade erg abstract, bijvoorbeeld wanneer het gaat over het vertroebelen van het maatschappelijke debat of het bijdragen aan polarisering (**Hill & Weulen Kranenbarg** en **Van der Vegt**). In alle gevallen gaat het echter ook om het risico op fysiek geweld als gevolg van online uitingen.

Bij twee bijdrages in dit themanummer zien we dat er een meer concrete link is tussen het online gedrag, in dit geval het delen van misbruikmateriaal (**Blokland et al.**) of de blootstelling aan online seksuele of gewelddadige content (**Notté et al.**), en offline fysieke gevolgen, in dit geval voor het misbruikte kind of de online veiligheid van kinderen meer in het algemeen. Hierbij geldt dan ook een sterkere maatschappelijke afkeer, hetgeen een verklaring biedt voor de duidelijkere strafbaarstelling van dergelijke online gedragingen. Desondanks zien we die maatschappelijke afkeer ook, weliswaar in mindere mate, bij online gedrag waarvan niet heel duidelijk wetenschappelijk is vastgesteld dat het ook tot fysiek geweld leidt. We zien dit terug in de bijdrage van **Van der Vegt**, maar ook nadrukkelijk in de maatschappelijke ophef rondom drill. De veelvuldige verwijzingen naar geweld in de muziek van deze rappers worden als ongewenst gezien, omdat de verwachting is dat deze online uitingen van geweld zullen resulteren in fysiek geweld. Diverse studies concluderen echter dat het geweld dat door drillrappers op sociale media tot uitdrukking wordt gebracht, gezien moet worden als performatief: meer gericht op het communiceren van een gevaarlijk en gewelddadig imago dan op een daadwerkelijke bereidheid tot het plegen van fysiek geweld (Ilan, 2020; Lane, 2019; Stuart, 2020; Roks & Van den Broek, 2020). Lang niet al het geweld dat online wordt gecommuniceerd in de drillrapcultuur resulteert dan ook in geweldsincidenten en studies wijzen er zelfs op dat sociale media door jongeren worden gebruikt om conflicten op een niet-gewelddadige manier te beslechten (zie o.a. Lane & Stuart, 2022).

De (maatschappelijke) verwachting dat het online gedrag ook offline negatieve gevolgen heeft, zorgt ervoor dat wij als criminologen vinden dat deze fenomenen ook door ons onderzocht moeten worden. Vaak is het echter heel lastig om te bepalen hoeveel impact het online gedrag daadwerkelijk heeft op het offline leven en in hoeverre beïnvloeding van dit online gedrag die offline schade kan voorkomen. Dit roept vragen op als: Wanneer zijn complottheorieën van substantieel belang in online berichten? Hoeveel invloed heeft een enkele tweet op het doen en laten van mensen, en vanaf hoeveel tweets vinden we dat er significante invloed van uitgaat?

Hoeveel mensen laten hun gedrag substantieel beïnvloeden door online platforms? Dit zijn vragen waar wij als criminologen niet alleen een antwoord op kunnen vinden en het zijn bovendien vragen die niet per definitie over criminaliteit gaan. Hierbij moeten we dan ook de kennis uit andere vakgebieden gebruiken.

Interessant voor de criminologie specifiek is dat alle papers gaan over spanningsvelden die online tot uiting komen. We zien spanning tussen wat we als maatschappij wel en niet willen accepteren of crimineel vinden en spanning tussen belangen van verschillende partijen. Maar ook spanning tussen vrijheid van meningsuiting en (schadelijke) uitingen die we willen inperken. Ook zien we spanning tussen wat we een kritische houding richting de wetenschap noemen en complotdenken of wetenschapsontkenning. Al deze spanningsvelden zorgen ervoor dat er heftige online en offline communicatie ontstaat waaruit uiteindelijk ook fysiek geweld kan ontstaan. De online platforms waarop deze spanningen tot uiting komen, zorgen ervoor dat de berichten snel worden verspreid en zo een groot publiek kunnen bereiken, dat hierdoor beïnvloed kan worden.

Op al deze online platforms zorgen de gebruikers voor het succes en de inhoud van de platforms. Zij bepalen wat hierop wordt gepost, geliket en gedeeld. In het paper over authenticiteit in de Nederlandse online drillcultuur (**Roks et al**.) wordt aangehaald dat er op deze platforms tegenwoordig sprake is van 'prosumenten' (Yar, 2012). In dit geval gaat het dan specifiek om gebruikers van online platforms die zowel zelf drillcontent maken (produceren) als deze ook van anderen bekijken (consumeren). Dit fenomeen is eerder ook geobserveerd als het gaat om online beeldmateriaal van seksueel kindermisbruik (Van der Bruggen & Blokland, 2021), zoals dat ook in de bijdrage van **Blokland et al**. aan bod komt. Hoewel niet expliciet vermeld, zien we dit ook terug bij het andere online gedrag dat in dit themanummer naar voren komt. Personen die zelf misinformatie of complottheorieën van anderen zien, kunnen hier zelf aan bijdragen door er hun eigen draai aan te geven. Of kinderen kunnen (seksueel) beeldmateriaal van leeftijdsgenoten, bijvoorbeeld middels gebruik van AI, aanpassen of in een andere context gebruiken en verspreiden. Wij observeren echter ook dat er naast producenten en consumenten nog een belangrijke groep is wanneer het gaat om online content, de personen die dit liken en delen. In de bijdrage van **Blokland et al**. wordt expliciet vermeld dat slechts een klein deel van de gebruikers een groot deel van de inhoud plaatst. Vermoedelijk geldt dit ook voor veel andere vormen van ongewenst online gedrag. Slechts een kleine groep maakt de schadelijke content, waarna de gebruikers van de platforms deze verder verspreiden en het 'succes' bepalen.

Kortom, er lijken inhoudelijk dus best wat overkoepelende bijzonderheden te zijn wanneer we kijken naar ongewenst online gedrag. Ondanks deze overeenkomsten zien wij dat er opvallend weinig overlap is in de gebruikte theoretische kaders in de artikelen in dit themanummer. Hoewel het gedrag plaatsvindt in de digitale context, vertrekken de auteurs vooral vanuit de theorieën die van oudsher worden gebruikt om specifiek gedrag te verklaren. In de bijdrage van **Blokland et al**. probeert men daarentegen juist de omgang met illegale online content (in dit geval beeldmateriaal van seksueel kindermisbruik) te toetsen aan verwachtingen op basis van theorieën over legale online content. Hierbij valt op dat de resultaten lang niet altijd in lijn zijn met deze verwachtingen en dat dergelijke illegale content dus

tot ander gedrag leidt. Vergelijkbare resultaten vinden we in heel ander eerder onderzoek naar cybercriminaliteit over illegale advertenties voor gehackte account credentials (Madarie et al., 2023). In dit onderzoek werd ook gevonden dat gebruikers van dergelijke illegale content zich niet hielden aan de gedragspatronen die we verwachten op basis van theorieën over legaal online consumentengedrag. Deze overeenkomst laat zien dat het belangrijk is om in onderzoek naar ongewenst online gedrag het theoretische perspectief te verbreden en ook te kijken naar online fenomenen die wellicht heel anders lijken te zijn, maar die gebruik maken van dezelfde online context. Dit onderschrijft ook de eerdergenoemde observatie van de NVC Cybercrime Divisie dat de kennis over digitalisering en criminaliteit breder moet worden uitgedragen en niet meer enkel van belang is voor de kleine groep onderzoekers die zich bezighoudt met cybercriminaliteit.

Onderzoek op basis van digitale artefacten

Online gedrag wordt vaak op een andere manier onderzocht dan offline gedrag. Hoewel ook onderzoek naar cybercriminaliteit veelvuldig gebruik maakt van klassieke methoden zoals surveys of dossieronderzoek, worden er ook heel vaak analyses uitgevoerd op digitale artefacten van het bestudeerde gedrag (zie voor overzichten Holt, 2023; Weulen Kranenbarg & Van 't Hoff-de Goede, 2023; Van der Wagen et al., 2024). Vaak gaat het dan om een analyse van verschillende vormen van online communicatie. De fenomenen die in dit themanummer worden belicht zijn, op het artikel over online veiligheid na (**Notté et al**.), onderzocht aan de hand van deze digitale artefacten. De online context biedt nieuwe mogelijkheden voor het observeren van gedrag, die offline niet bestaan.

Desondanks is het wel belangrijk om zich te realiseren dat de online communicatie van mensen wellicht lijkt op offline gedrag en communicatie, maar dat deze wel degelijk anders is. Over het algemeen hebben mensen meer invloed op de manier waarop ze hun online communicatie vormgeven, bijvoorbeeld doordat de reactie later gegeven kan worden. Daardoor kun je erover nadenken of en hoe je precies zal reageren op een tweet. Ook kun je zelf vormgeven hoe je online persoon neergezet wordt. De manier waarop iemand zich online gedraagt, hoeft dus niet per se gelijk te zijn aan de manier waarop die persoon zich offline gedraagt. Deze tegenstelling kan van belang zijn in het maatschappelijke debat over de mate waarin dit gedrag ongewenst is, zoals in het geval van de online drillrapcultuur (**Roks et al**.). Daarnaast heeft online communicatie ook bepaalde kenmerken die sterk afwijken van offline communicatie, waardoor de gevolgen heel anders kunnen zijn. Na een post van jou of over jou, is het over het algemeen lastig om hier nog volledige controle over te houden. Het blijft voor altijd op het internet staan en kan makkelijk door anderen worden gedeeld en gebruikt. Dit kan ook tot (onbedoelde) schade leiden.

Deze kenmerken van online gedrag maken het ook juist boeiend om dit te onderzoeken. Echter, wanneer er in onderzoek gebruik wordt gemaakt van digitale artefacten is het wel belangrijk om rekening te houden met de voor- en nadelen van dergelijke data. Ten eerste beperken veel onderzoeken zich vaak tot één bron van online communicatie. In het verleden, en ook in een aantal bijdrages in dit themanummer, was dit bijvoorbeeld Twitter (nu X). Deze voorkeur is niet vreemd, berichten op Twitter zijn over het algemeen goed toegankelijk en makkelijk vindbaar en

doi: 10.5553/TvC/0165182X2024066003001

het platform is lange tijd erg populair geweest. Ondanks dat veel mensen gebruik maken van Twitter, is dit echter wel een selectieve groep. Daarom moeten onderzoekers zich wel afvragen of dit voor hun onderzoeksonderwerp wel het meest relevante platform is. Ten tweede hebben recente ontwikkelingen ervoor gezorgd dat het platform minder populair is geworden en ook minder geschikt is voor onderzoek. Het socialemedialandschap raakt steeds verder gefragmenteerd, waardoor het als onderzoeker noodzakelijk is om eerst onderzoek te doen naar de platforms die voor het te bestuderen fenomeen het meest relevant zijn.

Een andere onderzoeksbenadering is de netnografie, zoals gebruikt in het artikel van **Roks et al**. Net als in de traditionele etnografische benadering staat 'being there' centraal en wordt gepoogd een fenomeen, gemeenschap of subcultuur met het gebruik van digitale technologie te onderzoeken. Ondanks dat 'being there' op het internet op een andere manier vormt krijgt, biedt de digitale wereld allerhande mogelijkheden om de etnografische onderzoeksbenadering online voort te zetten. De traditionele veldwerkrollen op het participant-observantcontinuüm kunnen online tenslotte ook worden uitgevoerd. Sociale media bieden immers verschillende functionaliteiten om te *lurken*, maar ook om actief en zichtbaar te participeren, onder andere door te reageren op *posts* en *comments* van andere gebruikers (Urbanik & Roks, 2020). Er kan hierbij ingezoomd worden op een specifiek platform zoals Telegram Messenger (zie o.a. Roks & Monshouwer, 2020), maar juist het bestuderen van hetzelfde fenomeen op meerdere socialemediaplatforms biedt vanwege de verschillende technische functionaliteiten interessante inzichten (zie ook **Roks et al**.).

Als derde beperking kan genoemd worden dat onderzoek naar ongewenst gedrag, alsook cybercriminaliteit zich vaak enkel richt op openbaar beschikbare communicatie. Dit geldt ook voor alle bijdrages in dit themanummer. Hierdoor wordt een belangrijk deel van de (een-op-een) online communicatie tussen personen gemist, omdat hiervoor vaak gebruik gemaakt wordt van privéberichten. Daardoor is het niet mogelijk het ongewenste online gedrag volledig in kaart te brengen. In onderzoek naar cybercriminaliteit is het inmiddels een aantal keer voorgekomen dat er wel inzicht was in privécommunicatie, bijvoorbeeld wanneer de politie een illegale darknetmarktplaats heeft overgenomen en zo ook de onderlinge communicatie en transacties heeft kunnen veiligstellen (Verburgh et al., 2018), of wanneer de onderlinge communicatie van ransomwaregroeperingen werd gelekt op het internet (Ruellan et al., 2023). Dit heeft nieuwe inzichten opgeleverd over de manier waarop daders met elkaar samenwerken, die niet konden worden gehaald uit de openbare communicatie tussen deze daders.

Ten vierde is het vaak niet mogelijk om te achterhalen wie er achter een online profiel schuilgaat. Het is ook goed mogelijk dat één persoon meerdere profielen heeft of dat één profiel juist door meer dan één persoon wordt gebruikt. Ook is er een vrijwel eindeloos aantal platforms waar de persoon mogelijk gebruik van maakt en die mogelijk relevant zijn om in onderzoek te betrekken. Vaak zijn er ook geen data beschikbaar over het offline gedrag van de bestudeerde personen of over hun percepties. Veelal worden er dan ook op basis van digitale artefacten aannames gedaan over de drijfveren van de personen die deze content posten, liken en delen.

Wat opvalt is dat hierdoor de noodzaak ontstaat om, mogelijk aanvullend, weer terug te gaan naar klassieke dataverzamelingsmethoden. Er lijkt een behoefte te zijn aan het interviewen van de posters, likers en delers van ongewenste online content. Wanneer het bijvoorbeeld gaat om het gedrag van jongeren op sociale media is het van belang om te weten hoe zij de content die ze voorbij zien komen beoordelen, en hoe ze hier vervolgens wel of niet op reageren. Aangezien wij als onderzoekers over het algemeen ouder zijn dan deze onderzoekspopulatie is het wellicht nodig dat we hen al betrekken bij het ontwerpen van ons onderzoeksdesign, om er zo voor te zorgen dat we de juiste vragen stellen of de juiste data verzamelen op de juiste plekken. Daarnaast zien we in de bijdrage van **Notté et al**. ook een duidelijke oproep om kinderen te betrekken bij discussies over hun online veiligheid.

Mogelijk levert het combineren van kwantitatief en kwalitatief onderzoek ook meer informatie op. Zeker wanneer AI-tools ons in de nabije toekomst de mogelijkheid geven om een grof totaalbeeld te krijgen, kan een aanvullende kwalitatieve analyse dat totaalbeeld wellicht verrijken en verder uitdiepen. Bij het gebruik van AI-tools moeten we er immers voor waken dat we het inzicht in de onderliggende data niet verliezen. Op het moment lijkt het echter nog lastig te zijn om kwalitatief en kwantitatief onderzoek echt met elkaar te integreren en niet als twee losse deelstudies te bespreken. Dat bleek ook tijdens het redactionele werk voor dit themanummer. Er is vaak een sterke behoefte aan kwalitatieve duiding van kwantitatieve resultaten en andersom is er een behoefte aan het kwantitatief schetsen van de ernst of grootte van een kwalitatief beschreven probleem. Hier ligt wellicht ook een taak voor de criminologieopleidingen in Nederland. Wanneer docenten erin slagen om studenten aan te leren (al dan niet AI-gegenereerde) kwantitatieve resultaten te duiden met kwalitatieve data en vice versa, dan kunnen zij wellicht een nieuw licht werpen op complexe digitale fenomenen.

Conclusie

De inleiding van dit themanummer maakt de criminologische relevantie van de bestudering van ongewenst gedrag online duidelijk. We merken op dat ons denken over digitale en online fenomenen veelal vertrekt vanuit de bekende binaire oppositie tussen online en offline en digitaal en fysiek, waarbij de zorgen rondom ongewenst gedrag online met name lijken te gaan over wat de gevolgen hiervan zijn voor de fysieke, offline wereld. De schadelijkheid van ongewenst gedrag online laat zich echter niet altijd makkelijk vaststellen en komt bijvoorbeeld tot uitdrukking in een toenemend gevoel van wantrouwen in de overheid, politiek of de wetenschap. Maar ook gevoelens van onveiligheid als gevolg van de blootstelling aan ongewenst gedrag online kunnen onder deze meer diffuse schadelijkheid worden geschaard. Lang niet altijd gaat het hier echter om online gedragingen die aangemerkt kunnen worden als criminaliteit, omdat we zien dat digitale ontwikkelingen zich sneller lijken te voltrekken dan de democratische processen die in staat zijn om online ongewenste gedragingen strafbaar te stellen.

doi: 10.5553/TvC/0165182X2024066003001

Voor criminologen genereert de voortschrijdende digitalisering van ons leven diverse digitale artefacten die bestudeerd kunnen worden op de openbaar toegankelijke delen van het internet en socialemediaplatforms. Hiervoor kan voor een deel gebruik worden gemaakt van de traditionele kwantitatieve en kwalitatieve onderzoeks- en analysemethoden, maar de digitale content leent zich ook voor een meer innovatieve en eigentijdse toepassing van de centrale beginselen van deze onderzoeksmethoden. De tussenkomst van veel verschillende digitale platforms, en met name de rol van de betrokken techbedrijven, maakt het echter wel (in toenemende mate) complex om een goed en volledig beeld te krijgen van online ongewenst gedrag en de gevolgen.

Het onderhavige themanummer maakt bovendien duidelijk dat het in het geval van ongewenst gedrag online gaat om onderwerpen die zich bevinden op een snijvlak tussen de criminologie en andere wetenschappelijke disciplines. Dit vraagt dan ook om een zekere mate van interdisciplinariteit of in sommige gevallen zelfs van transdisciplinariteit. Naar ons idee is daarvoor op dit moment geen aparte digitale criminologie of een andersoortige substroming binnen onze discipline nodig. Dit themanummer heeft immers laten zien dat er al een vrij grote verscheidenheid aan onderzoek is op dit gebied in Nederland. Enerzijds verwachten we dan ook dat vraagstukken waarin digitale technologie een rol van betekenis speelt in de nabije toekomst steeds breder opgepakt zullen worden door de criminologische gemeenschap, en dat onderzoek op dit gebied steeds vaker over meer zal gaan dan alleen cybercriminaliteit. Anderzijds verwachten we ook dat de voortschrijdende digitalisering op organische wijze zicht zal geven op de poreuze grenzen tussen het online en offline domein en de digitale en fysieke wereld in zowel criminologische fenomenen als de bestrijding hiervan. We verheugen ons nu al op het lezen van het resultaat van deze inspanningen in een toekomstig (digitaal) themanummer.

Literatuur

Bisschop, L. (2021). Daderschap in het antropoceen. *Tijdschrift voor Cultuur en Criminaliteit, 11*(1), 50-65.

boyd, d. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology, 10*(2), 223-244.

Centraal Bureau voor de Statistiek. (2023). *ICT, kennis en economie 2023*. Geraadpleegd op 24 september 2024, van https://longreads.cbs.nl/ict-kennis-en-economie-2023/

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*, 1-20.

Graham, R., Humer, S. G., Lee, C. S., & Nagy, V. (Eds.). (2024). *The Routledge international handbook of online deviance*. Routledge.

Hayward, K. J. (2012). Five spaces of cultural criminology. *The British Journal of Criminology, 52*(3), 441-462.

Hillyard, P., & Tombs, S. (2007). From 'crime' to social harm? *Crime, Law and Social Change, 48*(1-2), 9-25.

Holt, T. J. (2023). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior, 139*, Article 107493.

Ilan, J. (2020). Digital street culture decoded: Why criminalizing drill music is street illiterate and counterproductive. *The British Journal of Criminology, 60*(4), 994-1013.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2018). *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. WODC.

Lane, J. (2019). *The digital street*. Oxford University Press.

Lane, J. & Stuart, F. (2022). How social media use mitigates urban violence: Communication visibility and third-party intervention processes in digital urban contexts. *Qualitative Sociology*, 1-19.

Lavorgna, A. (2021). Looking at crime and deviancy in cyberspace through the social harm lens. In P. Davies, P. Leighton, & T. Wyatt (Eds.), *The Palgrave handbook of social harm* (pp. 401-420). Palgrave Macmillan Cham.

Leukfeldt, E. R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Eleven International Publishing.

Leukfeldt, E. R., & Roks, R. A. (2021). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior, 42*(11), 1458-1469.

Leukfeldt, E. R., & Weulen Kranenbarg, M. (2017). De menselijke factor in cybercrime. *Tijdschrift voor Criminologie, 59*(3), 282-290.

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitised world: On the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime, 22*, 324-345.

Lupton, D. (2014). *Digital sociology*. Routledge.

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.

Lusthaus, J., & Varese, F. (2021). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice, 15*(1), 4-14.

Lynch, M. J. (1990). The greening of criminology: A perspective for the 1990s. *The Critical Criminologist, 2*(3), 1-4.

Madarie, R., De Poot, C., & Weulen Kranenbarg, M. (2023). Criminal clickbait: A panel data analysis on the attractiveness of online advertisements offering stolen data. *Frontiers in Big Data, 6*, 1-15, Article 1320569. https://doi.org/10.3389/fdata.2023.1320569

Mooney, J. (2020). *The theoretical foundations of criminology. Time, place and context*. Routledge.

Negroponte, N. (1995). *Being digital*. Knopf.

Oerlemans, J. J., De Hingh, A., & Van der Wagen, W. (2024). Verschijningsvormen van gedigitaliseerde criminaliteit. In W. van der Wagen, J. J. Oerlemans, & M. Weulen Kranenbarg (Red.), *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (pp. 105-163). Boom.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. Routledge.

Roks, R. A., & Monshouwer, N. H. (2020). F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële verkenningen, 46*(2), 44-58.

Roks, R. A., & Van den Broek, J. B. A. (2020). *Cappen voor Clout? Een verkennend onderzoek naar Rotterdamse jongeren, drill en geweld in het digitale tijdperk*. Erasmus Universiteit Rotterdam.

Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2021). The hybridization of street offending in the Netherlands. *The British Journal of Criminology, 61*(4), 926-945.

Ruellan, E., Paquet-Clouston, M., & Garcia, S. (2023). Conti Inc.: Understanding the internal discussions of a large ransomware-as-a-service operator with machine learning. *arXiv preprint* arXiv:2308.16061

Schuilenburg, M. (2024). *Making surveillance public: Why you should be more woke about AI and algorithms*. Eleven Publishing.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a 'digital criminology'? *International Journal for Crime, Justice and Social Democracy, 6*(2), 17-33.

Stuart, F. (2020). *Ballad of the bullet. Gangs, drill music, and the power of online infamy*. Princeton University Press.

Urbanik, M. M., & Roks, R. A. (2020). GangstaLife: Fusing urban ethnography with netnography in gang studies. *Qualitative Sociology, 43*, 213-233.

Van der Bruggen, M., & Blokland, A. (2021). A crime script analysis of child sexual exploitation material fora on the Darkweb. *Sexual Abuse, 33*(8), 950-974. https://doi-org.vu-nl.idm.oclc.org/10.1177/1079063220981063

Van der Wagen, W. (2018). *From cybercrime to Cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory* [Proefschrift]. Rijksuniversiteit Groningen.

Van der Wagen, W., Oerlemans, J. J., & Weulen Kranenbarg, M. (2024). *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk*. Boom.

Van Erp, J., Stol, D. W., & Van Wilsem, J. (2013). Criminaliteit en criminologie in een gedigitaliseerde wereld. *Tijdschrift voor Criminologie, 5*(4), 327-341.

Verburgh, T., Smits, E., & Van Wegberg, R. (2018). Uit de schaduw: perspectieven voor wetenschappelijk onderzoek naar dark markets. *Justitiële verkenningen, 44*(5), 68-82. https://doi.org/10.5553/JV/016758502018044005006

Weulen Kranenbarg, M., & Van 't Hoff-de Goede, S. (2023). Online criminaliteit in criminologisch perspectief. Recente ontwikkelingen in het onderzoek naar daders en slachtoffers van online criminaliteit. *Tijdschrift voor Criminologie, 65*(4), 400-419.

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture, 8*(3), 245-260. https://doi.org/10.1177/174 1659012443227