Crime online

Lieve Lembrechts*

Jewkes, Y. (ed.) (2007). Devon: Willan Publishing

De wetenschappelijke interesse voor de relatie tussen media en criminaliteit is verre van nieuw. Één van de meest bestudeerde onderwerpen is de eventuele impact van gewelddadige en criminele media-inhouden op het publiek, of deze impact nu het ervaren van onveiligheidsgevoelens, het stellen van agressief en zelfs crimineel gedrag of andere effecten betreft (Potter, 1999, 25). Hoewel ook het internet vaak vanuit een dergelijke effectenoptiek bestudeerd wordt, lijkt het *world wide web* de interesse voor media en criminaliteit toch een nieuwe impuls gegeven te hebben. De vaststelling dat het internet gebruikt kan worden om criminaliteit te plegen, wijst er immers op dat het nieuwe medium niet alleen tal van kansen creëert, maar tevens een aantal bedreigingen inhoudt (Williams, 2006, 17). Waar oudere massamedia weliswaar ook aangewend kunnen worden om misdrijven - in het bijzonder persmisdrijven - te plegen, is hun instrumentele rol echter steeds eerder beperkt gebleven. Dat het internet een ruime waaier aan criminele doeleinden kan dienen, heroriënteert dan ook in aanzienlijke mate de studie van media en criminaliteit.
In *Crime Online* laat Jewkes in 11 hoofdstukken een aantal aspecten aan bod komen waarbij het plegen van criminaliteit door middel van het internet steeds de rode draad vormt. Doorheen het verzamelwerk wordt dit specifieke internetgebruik als een vorm van *cybercrime* beschouwd - zij het dat *cybercrime* hier niet tot beperkt is. Met dit werk wil Jewkes naar eigen zeggen tegemoet komen aan een wetenschappelijke leemte: *cybercrime* maakt naar haar mening immers vooralsnog onvoldoende voorwerp uit van wetenschappelijke en - in het bijzonder - criminologische reflecties (p.6). Dit zou niet alleen te maken hebben met de relatief jonge leeftijd van het internet, maar ook te wijten zijn aan de voorkeur die vele criminologen hebben voor de studie van criminaliteit in de 'echte' wereld (p.11). Het grootste probleem ligt volgens Jewkes dan ook in het feit dat cybercriminaliteit vaak onterecht als een aparte vorm van criminaliteit onderzocht wordt, los van 'aardse' vormen van criminaliteit. Vanuit die achtergrond wil *Crime Online* criminologen erop wijzen dat ze zich niet langer kunnen beperken tot het 'reële'; meer nog: dat met de komst van het internet de grens tussen het reële en het virtuele meer dan ooit vervaagt (p.11).

Met *Crime Online* is Jewkes niet aan haar proefstuk toe. Zo publiceerde ze reeds *Captive Audience: media, masculinity and power in prisons* (2002) waarin de rol van media in de constructie van identiteit besproken wordt en *Media and Crime* (2004), een overzichtswerk van onderzoek naar en theorievorming over de wijze waarop media criminaliteit (mee) construeren. Als voorloper van *Crime Online* verscheen *Dot.Cons: crime, deviance and identity on the internet* (2002), eveneens een verzamelwerk dat preciseert hoe de komst van het internet een impact heeft op het gedrag en de identiteit(svorming) van

* Leuvens Instituut voor Criminologie, K.U.Leuven.

de mens, ondermeer inzake gender en seksualiteit. In tegenstelling tot zijn voorloper wil *Crime Online* zich echter niet zozeer toespitsen op specifieke internetgerelateerde subthema's, maar een bredere blik bieden op de wijze waarop cybercriminaliteit zich voordoet en aangepakt wordt (p.5). De *cybercrime* die Jewkes aan bod laat komen, omvat trouwens uitsluitend die vormen van criminaliteit die reeds als criminaliteit gedefinieerd werden voor de komst van het internet - denk maar aan stalking en kinderpornografie - maar waarbij het gebruik van het internet een aantal voordelen biedt, zoals anonimiteit, snelheid en ruime verspreiding (p.4). Vormen van criminaliteit die ontstonden met de komst van en slechts kunnen bestaan dankzij het internet - zoals hacken en het doorsturen van virussen - worden niet besproken (Wall, 2003, xvii).
Jewkes beoogt echter geenszins louter de 'gevaarlijke' kant van het internet te bestuderen. De bredere blik die het boek wil bieden, bestaat er net in dat de dubbele aard van het medium benadrukt wordt. Internet is namelijk enerzijds weliswaar een medium dat perverteert, maar anderzijds ook een democratiserend medium, dat ons heel wat mogelijkheden biedt (p.5).

Crime Online is opgebouwd rond vier thema's: de definiëring, het plegen, de preventie en de aanpak van cybercriminaliteit. De definiëring en het plegen komen doorgaans samen aan bod, gezien de auteurs focussen op het idee dat *cybercrime* - net als andere criminaliteit trouwens - geconstrueerd wordt. Vanuit dat standpunt is *cybercrime* een vorm van criminaliteit geworden doordat bepaalde instanties of personen bepaalde gedragingen als crimineel gingen labellen. In een aantal hoofdstukken wordt benadrukt dat deze constructie niet steeds resulteert uit een 'natuurlijke' maatschappelijke dynamiek, maar doelbewust kan plaatsvinden. Centraal hierin staat hoe belanghebbenden - al dan niet via de klassieke media - een morele consensus trachten te creëren aangaande bepaalde gedragingen om zo tot (nieuwe) categorieën van criminaliteit te komen. De auteurs zochten hiervoor duidelijk inspiratie bij het morele paniekconcept van Cohen (1972), wat dan ook de rode draad doorheen een aantal hoofdstukken vormt.
Een eerste bijdrage die voortbouwt op de ideeën van Cohen, is die van Cere. Zij bespreekt hoe media en politici een morele paniekgolf veroorzaakten rond politiek getinte websites, die naar hun mening rellen zouden uitlokken, en uiteindelijk bekwamen dat deze webpagina's verboden werden. Cere legt uit dat het niet zozeer de politieke inhouden op zich waren die het voorwerp van de paniek uitmaakten als wel het feit dat het internet een belangrijke rol speelde in het verspreiden van dergelijke boodschappen.
Yar beschrijft vervolgens hoe de muziek- en filmindustrie het kopiëren van bestanden gecriminaliseerd en gelabeld heeft als 'illegaal downloaden'. De auteur schets de weg die deze industrie als *moral entrepreneur* aflegde om te komen tot de normatieve consensus dat dergelijke kopieeractiviteiten immoreel zijn, hoewel het haar in de eerste plaats om achterliggende economische motieven te doen is. Zoals wel vaker het geval is bij morele paniek, worden vooral jongeren hierbij geviseerd als grote boosdoeners.
Daar waar *moral entrepreneurs* zich relatief recent zijn gaan ontfermen over illegaal downloaden, gaat Fafinski in op een fenomeen dat de Britten al sinds het ontstaan van het voetbal bezighoudt: hooliganisme. Door de geschiedenis van voetbalgeweld te beschrijven, wil Fafinski duidelijk maken dat de paniek rond cyberhooliganisme - hooliganisme waarbij het internet aangewend wordt om de activiteiten te coördineren - eigenlijk oude wijn in nieuwe zakken is. Evenmin nieuw is de rol van de traditionele media hierin: deze media hebben hooliganisme immers niet alleen als probleem geconstrueerd, maar houden het ook in stand. Toch onderscheidt de morele paniek

waarvan bij cyberhooliganisme sprake is zich van de oudere paniek. Doordat, in het geval van cyberhooliganisme, de klassieke media het internet voorstellen als "a source of social evil" (p.125), wordt immers niet langer alleen de hooligan, maar het medium internet zelf als de *folk devil* aanzien.
Ook niet zo nieuw als het lijkt is cyberstalking. In haar bijdrage maakt Wykes duidelijk hoe stalking evolueerde van grensoverschrijdend naar crimineel gedrag in vele - zij het niet alle - rechtssystemen. Opnieuw blijken de media een belangrijke rol gespeeld te hebben om tot de consensus te komen dat stalking niet zomaar (deviant) gedrag vormt. Net als bij cyberhooliganisme, vervullen de media bij cyberstalking een bijzonder belangrijke rol in die zin dat niet alleen de stalker, maar ook het internet zelf als *folk devil* naar voor geschoven wordt. Interessant is de bedenking dat behalve de media ook meer wetenschappelijke bronnen aan de basis liggen van of bijdragen aan de constructie van (cyber)stalking, met als voorbeeld de victimologie. Door toedoen van victimologisch onderzoek kwam de focus volgens Wykes immers zo sterk op het slachtoffer te liggen dat er een klimaat van *victimism* ontstond, waarin de belangen van het slachtoffer sterk primeren (p.135). Eén van de neveneffecten van een dergelijk *victimism* is dat het slachtofferstatuut voor sommigen bijzonder aantrekkelijk gaat worden. Zonder te willen veralgemenen naar alle slachtoffers van (cyber)stalking gaat Wykes hierbij in op het voordeel dat *celebrities* kunnen halen uit hun slachtofferschap. Niet alleen blijkt het hebben van een stalker heel wat extra publiciteit op te leveren, maar staat de criminalisering van (cyber)stalking ook toe lastige paparazzi af te schudden. Dat bijvoorbeeld ongevraagd fotograferen als een vorm van stalking kan beschouwd worden, geeft beroemdheden de mogelijkheid om te bepalen wanneer en hoe ze al dan niet in beeld willen komen. Net zoals de muziek- en filmindustrie economisch voordeel haalt uit de criminalisering van downloaden, verwerven beroemdheden dan ook een zekere vorm van macht wanneer (cyber)stalking als misdrijf gelabeld wordt.
Waar sprake is van morele paniek, worden de media doorgaans als één van de katalysatoren van de paniekgolf beschouwd. Opvallend echter is de nadruk die doorheen het werk gelegd wordt op een specifiek medium, het internet, als voorwerp - en dus niet als aanstoker - van deze morele paniek. Drotner (1992) spreekt in een dergelijk geval van *media panic*. Hoewel nieuwe media - of het nu om televisie, stripverhalen of computergames gaat - historisch gezien steeds aanleiding gegeven hebben tot ongerustheid, vooral inzake de impact van deze media op kinderen en jongeren (Starker, 1991), is de ongerustheid in het geval van het internet ongemeen groot. Een mogelijke verklaring voor deze paniek ligt in het feit dat het internet, in tegenstelling tot de klassieke massamedia, lijkt te ontsnappen aan controlerende instanties zoals televisiezenders en het publiek een meer actieve rol geeft (Osgerby, 2004, 192).

Verder is een aantal hoofdstukken gewijd aan de preventie van *cybercrime*. Doorheen het werk wordt benadrukt dat preventie geen gemakkelijke opgave is en de inzet van verschillende partijen behoeft. Niet alleen internetproviders, de software-industrie en andere *architects of cyberspace* (p.25) dienen hun producten voldoende te beveiligen, maar ook internetgebruikers zelf moeten een aantal maatregelen nemen. In haar bijdrage schuift Brenner in dat kader een aantal bedenkelijke bevindingen naar voor. De auteur meent immers dat de internetgebruiker de "*responsibility not to become a victim*" heeft (p.23) en zelfs wettelijk verplicht is zichzelf te beschermen in cyberspace, wat weliswaar niet impliceert dat cybercriminelen van alle schuld vrijgepleit moeten worden. Naar haar mening is het bovendien vanzelfsprekend dat wie niet alle redelijke

beschermingsmaatregelen tegen *cybercrime* neemt en slachtoffer wordt, geen aanspraak maakt op enig reactief ingrijpen.
Hoewel doorheen het boek herhaaldelijk de verantwoordelijkheid van de gebruiker beaamd wordt, geeft Jewkes in haar inleidend hoofdstuk toe dat het voorstel van Brenner vrij extreem is (p.6). De veronderstelling dat we ons gedrag in cyberspace voortdurend rationeel in de hand kunnen houden, lijkt immers niet alleen onrealistisch te zijn, maar ook aan te zetten tot permanente - en uiteindelijk ongezonde - achterdocht ten aanzien van al wie via internet met ons in contact treedt. Doorheen de andere bijdragen wordt dan ook op een meer gematigde toon tot voorzichtigheid aangemaand. Finch en Smith, die beiden ingaan op identiteitsgerelateerde cybercriminaliteit, geven zo een aantal praktische en vooral haalbare tips, voornamelijk wat betreft het verstrekken van persoonlijke informatie via het internet. Zonder naar de bijdrage van Brenner te verwijzen, zet Yar trouwens een stevige kanttekening bij de intentie van preventiecampagnes waarin de nadruk gelegd wordt op het nemen van verantwoordelijkheid. Zo zou in de strijd tegen het illegaal downloaden van ouders verwacht worden dat ze verantwoordelijkheid voor hun kinderen opnemen, niet zozeer omdat kinderen moeten leren wat goed en kwaad is, maar omdat de ouders op die manier ingeschakeld kunnen worden in de logica van de *copyright* industrie en aldus bewakers worden van diens (economische) belangen (p.103-104). Ook Smith stelt de haalbaarheid van preventie in vraag. Hij merkt op dat het aanwenden van biometrische technologie om identiteitsgerelateerde *cybercrime* te voorkomen een keerzijde heeft; niet alleen hebben deze systemen een hoge kostprijs, maar ook doen ze vragen rijzen over het mogelijke risico op verplaatsing naar andere vormen van criminaliteit en op inbreuk op de privacy.

Hoewel het internet als nieuw medium dus ongetwijfeld aanleiding geeft tot ongerustheid, kan het ook tegen zichzelf gebruikt worden. In die optiek bespreekt Moore de rol van *computer forensics* in de bestrijding van cybercriminaliteit. Moore preciseert niet alleen hoe *computer forensics* een handig hulpmiddel vormt om *cybercrime* snel en grondig aan te pakken, maar ook meer en meer een absolute noodzaak lijkt te zijn, ondermeer op het vlak van bewijsgaring. Moore benadrukt echter wel dat het geen wondermiddel is: *cybercrime* blijkt dan ook ondanks - of net dankzij - de constante technologische vooruitgang vaak moeilijk aan te pakken, niet in het minst omdat cybercriminelen politie en justitie steeds een stapje voor zijn en deze laatste niet steeds de nodige degelijke opleiding krijgen (p.92).
Aas preciseert in haar bijdrage dat de moeizame bestrijding van *cybercrime* ook te wijten is aan een foute inschatting van het fenomeen. Doordat cybercriminaliteit de echte en virtuele wereld in elkaar doet vloeien, zijn de gevestigde interventies, gebaseerd op een opdeling tussen beide werelden, immers niet langer hanteerbaar. Ook de internetgebruiker zelf kan trouwens een hindernis vormen bij de aanpak van *cybercrime*. De bestrijding ervan is immers in grote mate afhankelijk van de meldingsbereidheid van de gebruikers, die vaak als eersten in contact komen met de vele verborgen vormen van *cybercrime*. Hun hulp is dan ook noodzakelijk, maar blijkbaar niet steeds zo vanzelfsprekend. Zo menen Jewkes en Andrews dat kinderpornografie op het internet zo moeilijk te bestrijden valt omdat de meeste surfers zich het lot van een onbekend kind niet lijken aan te trekken (p.75).

Het moge duidelijk wezen dat *Crime Online* cybercriminaliteit in haar ruimere context wil plaatsen. Dat het boek een ruim scala aan *cybercrime* gerelateerde thema's aan bod laat komen, heeft echter zowel voor- als nadelen. Voordeel is dat het boek op die manier

duidelijk in de verf kan zetten hoe de komst van het internet een groot aantal implicaties heeft op verschillende vlakken. Door de link tussen *cybercrime* en zijn klassieke variant te leggen, slaagt het boek er ook in de concrete impact van het internet ter zake te duiden. Een ander voordeel bestaat erin dat een ruimere benadering van *cybercrime* toelaat specifieke en vaak moeilijke technische terminologie achterwege te laten. Jewkes belooft trouwens in haar inleidende hoofdstuk een weinig technisch werk samengesteld te hebben. Hoewel de bijdrage van Moore inzake *computer forensics* op het randje van het verstaanbare balanceert voor computerleken, wordt deze belofte inderdaad ingelost. De keerzijde van de medaille is echter dat geen van de vele thema's die aan bod komen degelijk uitgespit wordt, hoewel de morele paniekdiscussie of het preventieluik op zich met gemak een volledig boek kunnen vullen. Het werk geeft dan ook soms de indruk (te) veel aan bod te willen laten komen, maar daarbij de rode draad doorheen het verhaal te verliezen.

Ook los van deze bedenking komt het verzamelwerk niet helemaal tegemoet aan de verwachtingen. Ondanks de vooropgestelde doelstelling komt immers de positieve kant van het internet - behalve in het kader van *computer forensics* - zelden aan bod. Het werk tracht weliswaar de perverterende kant van het internet te relativeren door erop te wijzen dat *cybercrime* onderhevig is aan definiëring en aansluit bij 'aardse' vormen van criminaliteit, maar dit betekent geenszins dat de democratiserende kant waarvan in de inleiding sprake is, aandacht krijgt. Opvallend is ook dat bepaalde vormen van cybercriminaliteit - vooral cyberstalking en cyberhooliganisme - soms net iets te veel in de marge van de reeds bestaande tegenhanger behandeld worden.

Toch laat het geen twijfel dat dit boek een aanrader is, niet alleen omwille van het actuele thema, maar ook omdat het de relativiteit van criminaliteit en het belang van de context waarin criminele gedragingen ontstaan, benadrukt.

Bibliografie

Cohen, S. (1972). *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*. Oxford: Blackwell.

Drotner, K. (1992). Modernity and media panics. In M. Skovmand & K.C. Schrøder (eds.), *Media cultures: reappraising transnational media* (pp. 42-62). Londen: Routledge.

Jewkes, Y. (2002). *Captive Audience: media, masculinity and power in prisons*. Cullompton: Willan.

Jewkes, Y. (ed.) (2002). *Dot.Cons: crime, deviance and identity on the internet*. Cullompton: Willan.

Jewkes, Y. (2004). *Media and Crime*. Londen: Sage.

Osgerby, B. (2004). *Youth media*. Londen: Routledge.

Potter, W.J. (1999). *On media violence*. Londen: Sage.

Starker, S. (1991). *Evil Influences: Crusades against the Mass Media*. New Brunswick: Transaction Publishers.

Wall, D.S. (ed.) (2003). *Cyberspace Crime*. Aldershot: Ashgate.

Williams, M. (2006). *Virtually criminal. Crime, deviance and regulation online*. Londen: Routledge.