WAT OFFLINE NIET MAG, MAG OOK ONLINE (SOMS) NIET
Internetexceptionalisme als bescherming voor de uitingsrechten van gebruikers

Michael Klos ▪

Samenvatting | Wat offline niet mag ook online niet. De Nederlandse en Uniewetgever drukken steeds vaker uit dat het normenkader op onlineplatforms gelijk is aan de offlinewereld. Hoewel de Nederlandse wetgever in het geval van doxing heeft gekozen voor een strafbaarstelling wordt desinformatie binnen de EU enkel online gereguleerd. Ook de digitaledienstenverordening volgt een exceptionalistische benadering waarbij, bijvoorbeeld, tussen onlineplatforms en zeer grote onlineplatforms wordt gedifferentieerd. Deze bijdrage bespreekt deze exceptionalistische benadering en laat zien dat het in het belang van de vrijheid van meningsuiting (zowel online als offline) kan zijn om te differentiëren tussen online en offline normstellingen.

Trefwoorden | [internetexceptionalisme], [vrijheid van meningsuiting], [digitaledienstenverordening], [onlineplatforms], [inhoudsmoderatie], [doxing]

DOI | 10.54195/NTM.19346

1 Inleiding

Mag wat offline niet gezegd mag worden, online niet gepost worden? Binnen de Europese Unie (EU) lijkt dit inderdaad het uitgangspunt.[1] Hierbij wordt steeds vaker expliciet een directe link gelegd met de mensenrechten van gebruikers.[2] Ook binnen Nederland wordt dit mantra 'wat offline niet kan, ook online niet' herhaald. Bijvoorbeeld door de politie.[3] Dit heeft uiteraard ook consequenties voor het balanceren van mensenrechten. Waar door de relatieve anonimiteit op het internet uitingsrechten vergaande feitelijke bescherming genoten, werden de privacyrechten van mensen die geraakt worden deze uitingen vaak minder goed geeffectueerd. De bescherming van de rechten van mensen en publieke belangen die geraakt worden door online uitingen heeft de laatste tijd meer aandacht. Dit uit zich bijvoorbeeld in de strafbaarstelling van het openbaar maken van persoonsgegevens met het doel om te intimideren (*doxing*).[4]

'Wat offline niet kan, kan ook online niet' kan als volgt worden opgevat: het normenkader is gelijk van toepassing op offline en online uitingen. Je mag elkaar niet bedreigen op straat

▪ Mr. Dr. M. Klos is als Universitair Docent verbonden aan de afdeling Encyclopedie van de Rechtswetenschap (Universiteit Leiden).

1 Zie de Europese verklaring 2023 over digitale rechten en beginselen voor het digitale decennium; Raad van de EU, 'Wat offline illegaal is, moet dat online ook zijn: standpunt Raad over wet digitale diensten', *Raad van de Europese Unie*, 21 september 2021, beschikbaar op https://consilium.europa.eu/nl/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act.

2 Art. 1 Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (*digitaledienstenverordening*).

3 Politie, 'Wat is er allemaal strafbaar online?', *vraaghetdepolitie.nl*.

4 Ministerie van Justitie en Veiligheid, 'Nieuwe wet tegen doxing "Je staat er niet alleen voor!"', *Rijksoverheid*, 2 januari 2024, beschikbaar op https://rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/het-verhaal-van-j-en-v/2024/nieuwe-wet-tegen-doxing-je-staat-er-niet-alleen-voor.

en dus ook niet per e-mail. Ook de aanpak hiervan is gelijk: je kan strafrechtelijk vervolgd worden voor het eerste feit (bedreiging op straat) en voor het tweede feit (bedreiging per e-mail). Justitie is 'blind' ten aanzien van de vraag of het feit offline of online is gepleegd. Het drukt uit dat gedrag op het internet niet bijzonder is en even strafwaardig is. Wat offline niet kan, kan ook online niet.

Hoewel dit klinkt als een logisch uitgangspunt zitten er toch wat haken en ogen aan. In dit artikel wordt dit uitgangspunt kritisch onderzocht. Centraal staat de vraag in hoeverre bij de aanpak van schadelijke inhoud gedifferentieerd dient te worden door overheden in de regulering van gedrag op onlineplatforms enerzijds en offline gedragingen anderzijds gelet op het recht op vrijheid van meningsuiting.

De focus ligt hierbij op overheidsactoren die een rol hebben in het reguleren van onlineplatforms. Het gaat daarbij in de eerste plaats om de wetgever in formele zin, maar ook om bijvoorbeeld de Europese Commissie die bindende gedragscodes kan afspreken met aanbieders van onlineplatforms. Bij de beantwoording van deze onderzoeksvraag wordt gefocust op twee categorieën van schadelijke inhoud die recentelijk een (hernieuwde) aanpak hebben gekregen: 1) desinformatie en 2) *doxing*. Deze categorieën zijn gekozen omdat het hierbij gaat om gedrag dat kan resulteren in zowel online en offline inhoud. Het gaat dus niet om uitingen die naar de aard alleen online of offline kunnen plaatsvinden.

Differentiatie in de toepassing van wetgeving op onlineplatforms en offline gedragingen wordt 'internetexceptionalisme' genoemd. Eric Goldman omschrijft internetexceptionalisme als 'het opstellen van internetspecifieke wetten die afwijken van de regelgevende precedenten in andere media.'[5] Daarbij kan in eerste instantie gedacht worden aan een strengere aanpak, maar het tegendeel kan ook waar zijn. In deze bijdrage wordt daarom de volgende specificering aangebracht: het gaat in deze bijdrage niet alleen om de juridische normstelling, maar ook om hoe deze normstelling zicht vertaalt in de aanpak van schadelijke inhoud. Ik gebruik daarbij nadrukkelijk het woord schadelijk en niet illegaal of onrechtmatig omdat door onlineplatforms vaak ook niet-illegale inhoud kan worden aangepakt onder de gebruikersvoorwaarden. Dit is ook het moment dat het recht op vrijheid van meningsuiting nadrukkelijk om de hoek komt kijken. Daarbij moet worden opgemerkt dat inhoud weliswaar zowel online als offline als schadelijk wordt gezien, maar dat de aanpak (bijvoorbeeld prioritering en mogelijke remedies) alsnog kan verschillen. Met andere woorden: zeker bij niet-illegale inhoud kunnen onlineplatforms ook kiezen voor uitingsvriendelijke remedies.[6]

Dit artikel bespreekt de onderzoeksvraag in drie delen. In het eerst deel wordt de twee-werelden-één-kadertheorie besproken die in de scheiding tussen online en offline inhoud besloten ligt. Door een verschil aan te brengen tussen een online en offlinewereld wordt ervan uitgegaan dat er twee verschillende 'werelden' zijn waar verschillende normen, regels en dus ook wetten van toepassing *kunnen* zijn. Het beschermen van uitings- en informatierechten van gebruikers van onlinediensten staan in deze discussie centraal. Zoals wordt besproken werd (vooral) in

5 In het Engels: '[…] crafting Internet-specific laws that diverge from regulatory precedents in other media.' zie E. Goldman, 'The Third Wave of Internet Exceptionalism', in B. Szoka & A. Marcus (red.), *The Next Digital Decade: Essays On The Future Of The Internet*, Washington, D.C.: TechFreedom 2010, p. 165.

6 E. Goldman, 'Content Moderation Remedies', *Michigan Technology Law Review* (28) 2021, afl. 1, doi:10.36645/mtlr.28.1.content, p. 7-9.

de jaren 1990 wetgeving vanuit staten benaderd met het idee dat deze een gevaar opleverde voor de 'internetrechten' van gebruikers.

Het tweede deel van dit artikel ziet op de exceptionele ingrepen die de (Unie)wetgever heeft gedaan op de regulering van onlineplatforms. Deze EU-wetgeving wordt vergeleken met de wetgeving in de Verenigde Staten van Amerika (VS) die in de jaren 1990 de aanzet gaf tot internetregulering. De digitaledienstenverordening is in 2022 aangenomen en is volledig van toepassing geworden op 17 februari 2024. De digitaledienstenverordening bouwt voort op de Richtlijn inzake elektronische handel[7] uit 2000 en moet dus ongeveer twee decennia aan ontwikkelingen op het gebied van onlineplatforms goedmaken. Om een voorbeeld te geven: Facebook (2004),[8] Twitter (nu: X) (2006)[9] en het Nederlandse Hyves (2004)[10] bestonden nog niet. Grootschalige onlineplatforms zoals wij die nu kennen waren er dus nog niet. Deze onlineplatforms functioneren als een 'tussenpersoon' in het gevolg geven aan nationale regulering. Ik sluit hierbij aan bij de definitie van de digitaledienstenverordening. Het gaat hierbij om een dienst die 'informatie opslaat en verspreidt bij het publiek'.[11] De focus ligt hierbij vooral op beeldbepalende onlineplatforms zoals YouTube, X en Instagram die onder deze verordening kwalificeren als zeer groot onlineplatform met een 'gemiddeld aantal maandelijks actieve afnemers van de dienst in de Unie bereiken dat gelijk is aan of groter is dan 45 miljoen'.[12] Deels omdat de regulering van deze onlineplatforms uniek te noemen valt in vergelijking met andere jurisdicties zoals in de VS, maar ook omdat deze onlineplatforms de diensten zijn die veel gebruikers in gedachten zullen hebben als het gaat om de aanpak van schadelijke inhoud.

In het derde deel worden twee recente ontwikkeling met betrekking tot de regulering van inhoud op het internet besproken. Daarbij laat ik inhoud die slechts een online verschijningsvorm heeft buiten beschouwing (denk aan deepfakepornografie). In plaats daarvan bespreek ik een categorie inhoud die een strafrechtelijke aanpak heeft gekregen die zowel online als offline van kracht is (*doxing*) en een categorie inhoud die alleen online wordt gereguleerd (desinformatie). Beide fenomenen kennen een duidelijke online dimensie, maar kennen (historisch) ook offline verschijningsvormen.

Dit artikel sluit af met een aanbeveling voor meer differentiatie om juist het normenkader zowel online als offline te versterken. Niet omdat het twee verschillende werelden zijn, maar omdat online en offlinecommunicatie verschillende specifieke kenmerken, en dus ook risico's, kennen.

7 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (*Richtlijn inzake elektronische handel*).

8 I. Lapowsky, '15 Moments That Defined Facebook's First 15 Years', *Wired*, 4 februari 2019, beschikbaar op https://wired.com/story/facebook-15-defining-moments.

9 M. Arrington, 'Odeo Releases Twttr', *TechCrunch*, 15 juli 2006, beschikbaar op https://techcrunch.com/2006/07/15/is-twttr-interesting.

10 A. Wokke & J. Schellevis, 'Uitgekrabbeld: de opkomst en ondergang van Hyves', *tweakers*, 31 oktober 2013, beschikbaar op https://tweakers.net/reviews/3307/all/uitgekrabbeld-de-opkomst-en-ondergang-van-hyves.html.

11 Art. 3 onder i Verordening (EU) 2022/2065.

12 Art. 33 lid 1 Verordening (EU) 2022/2065.

2 Twee werelden, één kader? Een normatieve aanzet voor internetexceptionalisme

De bescherming van mensenrechten op het internet houdt expliciet verband met de positie van het internet tegenover (nationale) staten. In 1996 bepleitte John Perry Barlow de digitale wereld van de jurisdictie van territoriale staten losgekoppeld te houden. In *A Declaration of the Independence of Cyberspace* brak hij een lans voor zelfbestuur van het internet. Inmenging van statelijke overheden wees hij nadrukkelijk af.[13] De context van deze verklaring was sterk gericht tegen paniekerige wetgeving om auteursrechten en de goede moraal van kinderen te beschermen. Niet zonder reden: in de VS bleek een deel van deze aangenomen wetgeving zelfs onconstitutioneel.[14]

Twintig jaar na deze verklaring bleef Barlow in een interview met *Wired* in 2016 bij dit punt: staten hebben geen jurisdictie over het internet omdat het internet niet samenvalt met territoriale grenzen.[15] Barlow accepteerde geen Leviathans (soevereine staten) op het internet. Eveneens zou Barlow niet heel blij zijn geweest met de zeer grote onlineplatforms die zijn uitgegroeid tot heuse Behemoths, de commerciële evenknie van de Leviathans. In beide gevallen is er sprake van regulering van bovenaf met weinig ruimte voor de onlinegemeenschap. Zelfbestuur hield ook in dat gemeenschappen op het internet zelf de wetten schreven.[16] Hoewel Barlow zijn *Declaration* anno nu moeilijk als blauwdruk kan gelden voor de verhouding tussen staat en platform, ademt de verklaring dat het internet exceptioneel is. Barlow zijn *Declaration* is dus een sterk voorbeeld van internetexceptionalisme waarbij de mensenrechten op het internet voornamelijk beschermd worden door deze tegen (statelijke) inmenging te beschermen.

Internetexceptionalisme houdt onder meer in dat het (gedrag op) internet gereguleerd wordt in specifieke wetgeving die niet van toepassing is op offline gedragingen. Tijdens de opkomst van het internet is bijvoorbeeld ingegrepen op schendingen van auteursrechten,[17] de verspreiding van en toegang tot pornografie en de beschikbaarheid van ander 'obsceen' materiaal op het internet.[18] Deze ingrepen waren veelal toegesneden op het gebruik van het internet en gingen veel verder dan 'offline' ingrepen. Goldman noemt deze golf van internetregulering 'internet paranoia'.[19] Internetexceptionalisme (zoals van Barlow) drukt ook uit dat wetgeving niet onverkort van toepassing is op het internet. Wetgeving vereist – zo is de gedachte – minimaal een herinterpretatie om toegepast te kunnen worden op het internet. Het gaat hier nadrukkelijk niet alleen om wetgeving die Barlow terecht afdeed als irrelevant omdat het ziet op het stoffelijke karakter van bijvoorbeeld goederen. Barlow wilde dat gemeenschappen op het internet een eigen normenkader konden ontwikkelen, los van de territoriale overheden. In deze verklaring spelen mensenrechten een expliciete rol. Barlow: 'We are creating a world where anyone, anywhere

13 J. Barlow, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*, 8 februari 1996, beschikbaar op https://eff.org/nl/cyberspace-independence.
14 Supreme Court of the United States 26 juni 1997, 117 S.Ct. 2329, 2351 (*Reno/American Civil Liberties Union*).
15 A. Greenberg, 'It's Been 20 Years Since This Man Declared Cyberspace Independence', *Wired*, 8 februari 2016, beschikbaar op https://wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence.
16 Barlow, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*, 8 februari 1996, beschikbaar op https://eff.org/nl/cyberspace-independence.
17 §512. Limitations on liability relating to material online, 17 USCA § 512 (West 2010, Westlaw Next through PL 116-179).
18 Deze wetgeving was onderwerp van discussie in Supreme Court of the United States 26 juni 1997, 117 S.Ct. 2329 (*Reno/American Civil Liberties Union*).
19 Goldman 2010 (*supra* noot 5) p. 165-166.

may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.'[20]

De verhoudingen liggen op 'het internet' anno 2024 anders dan Barlow hoopte. Niet gemeenschappen, maar zeer grote onlineplatforms bepalen in belangrijke mate het normenkader op het internet, waarbij de rol van de staat steeds nadrukkelijker is geworden. Onlineplatforms hebben echter nog steeds een belangrijke rol in het tegengaan van schadelijke inhoud. Dit is mede veroorzaakt door de exceptionele positie die onlineplatforms hebben gekregen van staten. De aansprakelijkheidsregimes voor internettussenpersonen zijn een stuk vriendelijker dan voor traditionele media. Deze uitzonderlijke benadering van aansprakelijkheid moet in het achterhoofd gehouden worden wanneer het gaat om de aanpak van online inhoud. Hoewel deze benadering nog steeds in grote lijnen van toepassing is, zijn het deels ook (goed onderhouden) monumenten uit een verleden van internetoptimisme. Goldman noemt deze eerste golf van internetexceptionalisme zelfs internetutopisme.[21]

Deze monumenten zijn recentelijk nog wat opgepoetst en zelfs onderdeel geworden van nieuwe wetgevingsoperaties. Ik bespreek in dit verband de context van de VS en de EU gelet op hun relatieve belang voor de mensenrechten van gebruikers in Nederland. De meeste (en meest gebruikte) onlineplatforms hebben immers hun hoofdkantoor in de VS. In de VS zijn daarnaast duidelijke aanwijzingen van beide vormen van exceptionalisme.

3 Het exceptionele karakter van het internet

De eerste golf van internetexceptionalisme, zoals uiteengezet door Goldman, moet worden gezien als een product uit die tijd.[22] Zeker de benadering zoals deze door de wetgever is gekozen in de VS kan worden gezien als een duidelijke reactie op zeer vergaande aansprakelijkheid van internettussenpersonen en de betekenis hiervoor voor onder anderen de uitingsrechten van gebruikers.[23] Het is deze wetgeving waar de EU (en dus ook Nederland) zich aan kan spiegelen. Deze spiegel is des te relevanter omdat in de VS de impact op de uitingsvrijheid expliciet meespeelde (en speelt).

Door de bank genomen kan in wetgeving gekozen worden voor het volledig uitzonderen van aansprakelijkheid van internettussenpersonen (zoals in de VS voor een belangrijk deel het geval is), het volledig en direct aansprakelijk maken van internettussenpersonen (zoals in bijvoorbeeld China) en een conditionele aansprakelijkheid (zoals in de EU het geval is).[24] Daarbij moet worden opgemerkt dat alleen strikte aansprakelijkheid voor internettussenpersonen zich laat vergelijken met 'offline' redactionele controle. De rest is een vorm van 'exceptionalisme' omdat vergelijkbare offline media in vergelijkbare situaties zich niet aan aansprakelijkheid kunnen onttrekken. In deze bijdrage focus ik mij op het exceptionele karakter van deze regulering en

20 Barlow, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*, 8 februari 1996, beschikbaar op https://eff.org/nl/cyberspace-independence.
21 Goldman 2010 (*supra* noot 5) p. 165.
22 Goldman 2010 (*supra* noot 5) p. 165.
23 J. Kosseff, *The Twenty-Six Words That Created the Internet*, Ithaca: Cornell University Press 2019, p. 64-68.
24 T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*, New Haven: Yale University Press 2018, p. 33.

slechts beperkt op welke bescherming en verantwoordelijkheden onlineplatforms kennen onder de verschillende aansprakelijkheidsregimes.[25]

3.1 Internetexceptionalisme in de jaren 1990 en 2000

Het internetexceptionalisme in de VS komt echter niet uit de lucht vallen. Zoals opgemerkt was het een directe reactie op een rechtelijke uitspraak waaruit (volgens de wetgever) onwenselijke effecten voortkwamen. Wat in 1996 zou worden gecodificeerd als Sectie 230 van de *Communications Act* van 1934 (zoals geamendeerd bij de *Telecommunications Act* van 1996),[26] was een directe reactie op een uitspraak van de *New York Supreme Court* in 1995.[27] De naam van deze rechtbank moet overigens niet opgevat worden alsof deze rechter de hoogste rechter in New York is. Het gaat hierbij om een rechtbank in eerste aanleg.

De *New York Supreme Court* deed uitspraak in een civiele zaak aangespannen tegen wat het best valt te karakteriseren als een online prikbord. Op dit prikbord werd onder meer gediscussieerd over beurszaken. Enkele gebruikers lieten zich smadelijk uit over een beursmakelaarskantoor. Deze liet het hier niet bij zitten en stapte naar de rechter om de exploitant van het online prikbord voor de rechter te dagen. De rechter moest beoordelen of het online prikbord als een *publisher* (uitgever) functioneerde of dat het meer het karakter had als een doorgeefluik zonder redactionele controle. De rechter kwam tot de conclusie dat het onlineprikbord inderdaad functioneerde als een *publisher*. Het prikbord bepaalde de regels voor gebruikers en voerde ook wat moderatie uit waarbij dus redactie werd gevoerd op de inhoud. Juist het vaststellen van regels en het handhaven van deze regels zijn typische activiteiten van een *publisher*. Dat de exploitant van het onlineprikbord de gewraakte berichten niet had gezien deed niet af aan de redactionele controle die de exploitant uitoefent volgens de rechter.[28] Als redactie ben je niet enkel verantwoordelijk voor de inhoud die je toevallig kiest te controleren, maar voor alle inhoud.

Deze benadering zorgde voor een dilemma voor aanbieders van onlinediensten: elke vorm van toezicht en controle – hoe beperkt ook – zorgde al voor volle aansprakelijkheid voor alle inhoud geplaatst door gebruikers. Niet modereren was juridisch veiliger, maar uiteraard ook onbevredigend omdat andere schadelijke inhoud dan niet weggehaald zou worden. Aanbieders werden in feite juridisch gestimuleerd een *hands-off* benadering te volgen.[29] Een dergelijke terughoudende houding zorgt er ook voor dat schadelijke inhoud die bijvoorbeeld de privacy van anderen schendt niet actief wordt aangepakt. Een dienst die wel zou overgaan tot moderatie zou gestimuleerd kunnen worden juist veel meer weg te halen om aansprakelijkheid te voorkomen wat juist weer negatieve gevolgen heeft voor de uitingsrechten van gebruikers.

25 De bespreking van de aansprakelijkheid van internettussenpersonen is gebaseerd op M. Klos, *Wrongful Moderation: Regulation of Internet Intermediary Service Provider Liability and Freedom of Expression*, Leiden: Leiden University 2022. Zie ook F. Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*, Cheltenham: Edward Elgar Publishing 2020, doi:10.4337/9781839104831.

26 Over de citeerwijze van deze Sectie verschillen de meningen, zie B.E. Reid, 'Section 230 of… what?', *Blake E. Reid*, 4 september 2020, beschikbaar op https://blakereid.org/section-230-of-what.

27 New York Supreme Court 24 mei 1995, 23 Media L Rep 1794 (*Stratton Oakmont/Prodigy*).

28 New York Supreme Court 24 mei 1995, 23 Media L Rep 1794 (*Stratton Oakmont/Prodigy*).

29 Kosseff 2019 (*supra* noot 23) p. 55-56.

Zoals opgemerkt beantwoordde de wetgever dit in de VS met Sectie 230.[30] Daarbij is voor deze bespreking vooral (c)(1) van belang. Deze bepaling luidde (en luidt):

> **'(c) Protection for "Good Samaritan" blocking and screening of offensive material**
> **(1) Treatment of publisher or speaker**
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.'[31]

Op een paar uitzonderingen na (bijvoorbeeld federale strafwetgeving en auteursrechtelijk beschermd materiaal) konden (en grotendeels nog steeds kunnen) (gebruikers van) interactieve computerdiensten niet aansprakelijk worden gehouden als een *publisher* of *speaker* voor de inhoud aangeboden door derden.[32] In de praktijk betekent dit een zeer verstrekkende uitzondering voor aansprakelijkheid. Zo geeft Goldman het voorbeeld dat eenzelfde brief met onrechtmatige inhoud van een derde gepubliceerd in de papieren krant en op de online editie tot een verschillende uitkomsten leidt wat betreft de aansprakelijkheid. De krant is wel aansprakelijk voor de papieren variant, maar niet aansprakelijk voor de online variant.[33] De online krant kan gelet op de eigen aansprakelijkheid dus meer ruimte bieden aan derden dan de offline variant.

Deze vrijwaring van aansprakelijkheid komt de uitingsrechten van gebruikers in beginsel ten goede. Online media hoeven de inhoud immers niet te controleren voor publicatie. Anders dan offline media draagt het onlineplatform geen redactionele verantwoordelijkheid voor dergelijke inhoud. De plaatsing van (c)(1) onder het kopje 'Protection for "Good Samaritan" blocking and screening of offensive material' laat zien waar het de wetgever om te doen was: een onlineplatform die als Goede Samaritaan actie onderneemt tegen schadelijke inhoud moet niet opeens voor andere inhoud aansprakelijk worden gehouden. Sectie 230(c)(2)(A) zorgde voor het laatste beetje bescherming. Ook als aanbieders inhoud weghalen dat constitutioneel beschermd wordt, kunnen ze niet aansprakelijk worden gehouden zolang ze in goed vertrouwen konden aannemen dat het afkeurenswaardige inhoud betreft.[34]

Door Goldman wordt dit stukje wetgeving als typische exceptionele wetgeving opgevoerd.[35] Goldman rekent Sectie 230 tot de eerste golf van internetexceptionalisme: wetgeving waarin het internet volgens Goldman nog optimistisch en zelfs utopisch benaderd werd.[36] Door deze twee bepalingen krijgt de aanbieder van een onlineplatform dus een zeer brede ruimte van de wetgever om te bepalen wat voor inhoud wel en niet toegestaan is. Hierbij dient opgemerkt te worden dat aanbieders van onlineplatforms gemakkelijk hun handen kunnen aftrekken van

30 Kosseff 2019 (*supra* noot 23) p. 64-68.
31 §230. Protection for private blocking and screening of offensive material, 47 USCA § 230(c)(1) (West 2018, Westlaw Next through PL 116-91).
32 §230. Protection for private blocking and screening of offensive material, 47 USCA § 230(e) (West 2018, Westlaw Next through PL 116-91).
33 E. Goldman, 'An Overview of the United States' Section 230 Internet Immunity', in G. Frosio (red.), *The Oxford Handbook of Online Intermediary Liability*, Oxford: Oxford University Press 2020, doi:10.1093/oxfordhb/9780198837138.013.8, p. 162.
34 §230. Protection for private blocking and screening of offensive material, 47 USCA § 230(c)(2)(A) (West 2018, Westlaw Next through PL 116-91).
35 Goldman 2020 (*supra* noot 33) p. 162-163.
36 Goldman 2010 (*supra* noot 5) p. 165.

schadelijk gedrag op het internet. Ook als een dienstverlener bekend wordt met het schadelijke karakter van de inhoud hoeft de dienstverlener geen actie te ondernemen. Sectie 230 beschermt aanbieders tegen juridische gevolgen van moderatie, maar bevat geen aanmoediging om over te gaan tot moderatie.[37]

In de EU werd gekozen voor een minder verstrekkende uitzondering. Anders dan Sectie 230 werd de wetgeving in de EU geïnitieerd vanuit een andere zorg dan de angst voor oververwijdering. Binnen de EU zou nationale wetgeving het ondoenlijk maken voor aanbieders om hun diensten EU-breed aan te bieden. Het doel van de EU-wetgevingsoperatie was dus harmonisatie. Geen harmonisatie van materiele wetgeving, maar harmonisatie van een procedure: wanneer kunnen internettussenpersonen aanspraak maken op een uitzondering voor aansprakelijkheid voor inhoud aangeboden door derden?[38]

Voor diensten die door gebruikers aangeleverde informatie opslaat heeft de EU een conditionele uitzondering in het leven geroepen. Deze *safe harbour* houdt in dat zogenaamde hostingdiensten onder omstandigheden niet aansprakelijk kunnen worden gehouden voor inhoud geplaatst door derden. Hostingdiensten (waaronder ook onlineplatforms vallen) zijn volgens het eerste lid van artikel 14 van de Richtlijn inzake elektronische handel (2000) niet aansprakelijk voor inhoud van derden zolang ze a) geen kennis van het illegale karakter hebben en b) prompt handelen als ze deze kennis verwerven zolang zij niet te betrokken zijn bij de totstandkoming van deze inhoud.[39]

Naast deze veilige haven kende de Richtlijn ook een verbod voor lidstaten om internettussenpersonen te verplichten in het algemeen toezicht te houden op de dienst. Onlineplatforms kunnen onder artikel 15 niet verplicht worden alle inhoud geplaatst door gebruikers te controleren of op zoek te gaan naar de feiten en omstandigheden waaruit het illegale karakter van inhoud blijkt.[40] De verantwoordelijkheid van aanbieders was onder deze Richtlijn dus voornamelijk reactief en niet noodzakelijk proactief.[41] Aanbieders dienen te reageren op meldingen van dergelijke inhoud en actie te ondernemen wat resulteert in het ontoegankelijk maken van de betreffende inhoud.

Met de komst van de digitaledienstenverordening in 2022 is de Richtlijn geamendeerd. Artikel 14 en 15 uit de Richtlijn zijn vervangen door artikel 6 en artikel 8 van de Verordening.[42] Artikel 6 is daarmee komen te luiden:

> '1. Wanneer een dienst van de informatiemaatschappij bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, is de dienstaanbieder niet aansprakelijk voor de op verzoek van de afnemer van de dienst opgeslagen informatie, op voorwaarde dat de dienstaanbieder:

37 Klos 2022 (*supra* noot 25) p. 197-198.
38 Overweging 3 tot 8 Richtlijn 2000/31/EG.
39 Art. 14 Richtlijn 2000/31/EG. Zie ook HvJ EU 12 juli 2011, C-324/09, par. 116 en 119, *IER* 2011/58, m.nt. C. Gielen (*L'Oréal v. eBay*).
40 Art. 15 Richtlijn 2000/31/EG.
41 Al probeerde de EC onlineplatforms op dit punt gerust te stellen, zie Communication COM(2017)555 final van the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions van 28 september 2017 Tackling Illegal Content Online Towards an enhanced responsibility of online platforms. De digitaledienstenverordening doet hetzelfde in art. 7 Verordening (EU) 2022/2065. Zie ook Klos 2022 (*supra* noot 25), p. 132-150.
42 Art. 89 Verordening (EU) 2022/2065.

a) niet daadwerkelijk kennis heeft van de illegale activiteit of illegale inhoud en, wanneer het een vordering tot schadevergoeding betreft, geen kennis heeft van feiten of omstandigheden waaruit de illegale activiteit of de illegale inhoud duidelijk blijkt; of
b) zodra hij dergelijke kennis of dergelijk besef krijgt, prompt handelt om de illegale inhoud te verwijderen of de toegang daartoe onmogelijk te maken.'[43]

Kortgezegd is de regel nog steeds dat onlineplatforms niet aansprakelijk zijn voor onwettige inhoud geplaatst door derden zolang ze geen kennis hebben van deze inhoud of wanneer ze na een melding deze inhoud zo snel mogelijk verwijderen. Om te voorkomen dat onlineplatforms gedwongen kunnen worden alle inhoud te filteren en op deze wijze kennis krijgen van dergelijke inhoud is artikel 8 opgenomen in de digitaledienstenverordening. Deze luidt: '[a]an aanbieders van tussenhandeldiensten wordt geen algemene verplichting opgelegd tot monitoring van de door hen doorgegeven of opgeslagen informatie noch tot actief onderzoek naar de feiten of omstandigheden die duiden op illegale activiteiten.'[44]

Artikel 6 beperkt dus de aansprakelijkheid van onlineplatforms tot inhoud waar ze daadwerkelijk kennis van hebben terwijl artikel 8 de verantwoordelijkheid van onlineplatforms beperkt tot inhoud waarop zij worden gewezen. Onlineplatforms hoeven zelf niet op zoek te gaan naar (feiten en omstandigheden rondom) illegale inhoud. Het 'hart' van de Richtlijn uit 2000 is daarmee onverminderd actueel gebleven. De digitaledienstenverordening bouwt voort op de exceptionalistische benadering van de Richtlijn, maar complementeert deze met zorgvuldigheidseisen en transparantieverplichtingen. Het wel of niet voldoen aan deze eisen of verplichtingen tast echter niet een beroep op de *safe harbour* aan. Het niet voldoen aan deze zorgvuldigheidseisen en transparantieverplichtingen worden onderdeel van bestuursrechtelijk toezicht. De exceptionele uitzonderingen voor aansprakelijkheid van internettussenpersonen drukken uit dat onlineplatforms invloed kunnen uitoefenen op wat er gedeeld wordt op hun platforms, maar dat het (anders dan voor traditionele media) ondoenlijk is om verantwoordelijkheid te nemen voor alle inhoud die geplaatst wordt.

Kenmerkend voor deze benadering is dat het niet verplicht is de gebruiker te achterhalen die de duidelijk illegale inhoud heeft geplaatst. Daarbij verschilt de aansprakelijkheid van onlineplatforms van traditionele offline media zoals de uitgever en de drukker. Artikel 14 van de Richtlijn is in ons Burgerlijk Wetboek omgezet in artikel 6:196c. Ten eerste kent ons Burgerlijk Wetboek geen *safe harbour* voor drukkers en uitgevers.[45] Ten tweede heeft ons Wetboek van Strafrecht de uitzondering van strafbaarheid voor strafrechtelijke deelneming aan drukpersmisdrijven voor drukkers en uitgevers afhankelijk gemaakt van de mogelijkheid om respectievelijk de uitgever of auteur aan te spreken voor een strafbare uiting.[46] Onlineplatforms kunnen aan strafrechtelijke vervolging voor deelneming ontsnappen door gehoor te geven aan een bevel van de officier van justitie om de gewraakte gegevens ontoegankelijk te maken.[47] Wel moet worden opgemerkt dat in sommige gevallen een dergelijk bevel zinloos is (bijvoorbeeld als de

43 Art. 6 lid 1 Verordening (EU) 2022/2065.
44 Art. 8 Verordening (EU) 2022/2065.
45 Vergelijk met art. 6:196c BW.
46 Zie art. 53 en 54 Sr.
47 Zie art. 54a Sr. Zie voor de procedure van het bevel art. 125p Sv.

internettussenpersoon reeds op de hoogte is van het strafbare handelen van de gebruikers en hiertegen weigert op te treden) en dus ook niet nodig is om over te gaan tot vervolging.[48]

Voordat ik overga tot een bespreking van de internetexceptionalistische benadering van de digitaledienstenverordening maak ik eerst een uitstap naar Straatsburg. Het is onmiskenbaar dat het Europees Hof voor de Rechten van de Mens (EHRM) een stempel heeft gedrukt op internetregulering binnen de Europese context als het gaat om het balanceren van het recht op privacy tegen het recht op vrijheid van meningsuiting. Daarnaast geeft het EHRM als eerste een differentiatie van aansprakelijkheid tussen onlineplatforms gebaseerd op de grootte van het onlineplatform.

3.2 Internetexceptionalisme en het EHRM

Gelet op het systeem van het EVRM wordt het EHRM veelal geconfronteerd met zaken waarbij een balans moet worden gezocht tussen de vrijheid van meningsuiting (artikel 10) en privacyrechten van derden die worden getroffen door schadelijke inhoud (artikel 8) geplaatst door derden op onlineplatforms. *Delfi* (2015) en *MTE & Index.hu* (2016) geven samen een aardig beeld van de EHRM-benadering. Het EHRM differentieert hierbij allereerst tussen de inhoud waarmee de aanbieder wordt geconfronteerd. Wilman merkt hierover op dat het EHRM een verhoogde aansprakelijkheid aanneemt voor zeer duidelijke en schadelijke illegale inhoud.[49] Ten tweede differentieert het EHRM de aansprakelijkheid tussen platforms gebaseerd op de grootte en rol die het platform inneemt in het informatielandschap. Kleine non-profit partijen worden daarbij anders behandeld dan grote commerciële platforms.

Delfi en *MTE & Index.hu* illustreren deze exceptionalistische benadering waarbij het EHRM de grootte van het platform en het (commerciële) karakter van het platform expliciet meeweegt. In *Delfi* ging het om een groot commercieel nieuwsplatform. Onder een bericht met de titel '*SLK Destroyed Planned Ice Road*' werden op *Delfi* circa twintig duidelijke illegale bedreigingen gericht aan de meerderheidsaandeelhouder van het bedrijf SLK een exploitant van veerdiensten.[50] Delfi modereerde daarnaast uit eigen beweging ongepaste reacties en was ook de enige die dit kon: gebruikers die commentaren hadden achtergelaten konden deze niet later wijzigen/terugtrekken.[51] Van belang hierbij is dat de auteur van de reacties anoniem was voor de persoon die geraakt werd door de reacties.[52] Deze reacties waren daarnaast duidelijk illegaal.[53] *MTE & Index.hu* verschilt op dit punt, omdat het gaat om een non-profit organisatie (MTE) die een opiniestuk had geplaatst over onethische advertentiepraktijken op het internet. Deze werd doorgeplaatst door een commercieel internetplatform Index.hu. Onder dit bericht werden ook door gebruikers berichten geplaatst over deze advertentiepraktijken die volgens de adverteerder in een inbreuk maakte op hun eer en goede naam.[54]

48 Hof Den Haag 23 augustus 2023, ECLI:NL:GHDHA:2022:1550, *NJ Feitenrechtspraak Strafzaken* 2023/92.
49 Wilman 2020 (*supra* noot 25) p. 233-234.
50 EHRM 16 juni 2015, 64569/09, par. 16-18, 144 en 156 (*Delfi/Estland*).
51 EHRM 16 juni 2015, 64569/09, par. 145 (*Delfi/Estland*).
52 EHRM 16 juni 2015, 64569/09, par. 151 (*Delfi/Estland*).
53 EHRM 16 juni 2015, 64569/09, par. 153 (*Delfi/Estland*).
54 EHRM 2 februari 2016, 22947/13, par. 5-15 (*Magyar Tartalomszolgátatók Egyesülete (MTE) en Index.hu Zrt/Hongarije*).

In *Delfi* en *MTE & Index.hu* gaat het EHRM in op de omstandigheden waaronder internettussenpersonen aansprakelijk kunnen worden gehouden voor inhoud geplaatst door derden. In *Delfi* kwam de Grote Kamer tot het oordeel dat een schadevergoeding van 320 euro geen schending inhield van de vrijheid van meningsuiting van dit nieuwsportaal.[55] In *MTE & Index.hu* kwam een het EHRM tot een ander oordeel. In dit geval ging het overigens slechts over een proceskostenveroordeling. Het EHRM merkt echter op dat het rechtelijk oordeel waarover geklaagd wordt gebruikt kan worden voor nieuwe rechtszaken met het doel om schadevergoeding te verkrijgen.[56] Voor het EHRM was bepalend dat het in *MTE & Index.hu* niet ging om duidelijke illegale inhoud én dat MTE geen (grote) commerciële organisatie is (anders dan Index.hu), maar een kleine non-profit zonder economische belangen bij de inhoud.[57] In tegenstelling tot bij *Delfi* waar het EHRM vaststelde dat het gaat om een grote commerciële partij die daarnaast ook financieel te winnen heeft bij gebruikersreacties. Reacties leiden immers organisch tot meer aandacht voor nieuwsberichten en dus meer inkomsten.[58]

In *Delfi* sloot de Grote Kamer aan bij de positie van de Raad van Europa dat de aansprakelijkheid voor, en verantwoordelijkheid van, internettussenpersonen voor gebruikersinhoud ten opzichte van 'traditionele' uitgevers een gedifferentieerde en graduele benadering vereist.[59] Dit betekent allereerst dat 'traditionele' aansprakelijkheidsregimes voor bijvoorbeeld uitgevers of drukkers niet één op één kunnen worden gekopieerd naar, of worden toegepast op, internettussenpersonen. Het betekent ook dat de aansprakelijkheid voor gebruikersinhoud tussen verschillende aanbieders kan variëren.

Het hete hangijzer is daarbij vrijwel altijd de (relatieve) anonimiteit die wordt geboden aan gebruikers. De verdeling van aansprakelijkheid tussen de gebruikers en de aanbieder van een internetdienst was, en is, daarbij de kern van de discussie.[60] De Grote Kamer van het EHRM is er getuige *Delfi* niet toe geneigd om vergaande juridische beperkingen op de anonimiteit die het internet verschaft te accepteren met een beroep op het recht op privacy van mensen die geraakt worden door onrechtmatige uitingen van andere gebruikers. De Grote Kamer merkt zelfs op dat deze anonimiteit die gebruikers geboden wordt door het internet er juist voor zorgt dat mensen vrij hun ideeën kunnen delen zonder ongewenste aandacht of vergelding.[61] Daarbij kan worden opgemerkt dat het relativeren van anonimiteit op het internet door anonieme uitingen in te beperken ook invloed heeft op de rechten neergelegd in artikel 8 EVRM (het recht op privacy). Anonimiteit kan een gebruiker ook juist bescherming bieden tegen dergelijke uitingen – zeker als het om iemand gaat met een publiek profiel.

Het EHRM differentieerde de aansprakelijkheid dus in 2015 en 2016 tussen onlineplatforms al aan de hand van het karakter van het platform (groot en commercieel of een kleine non-profit?)

55 EHRM 16 juni 2015, 64569/09, par. 160-162 (*Delfi/Estland*).
56 EHRM 2 februari 2016, 22947/13, par. 86-91 (*Magyar Tartalomszolgátatók Egyesülete (MTE) en Index.hu Zrt/Hongarije*).
57 EHRM 2 februari 2016, 22947/13, par. 64 (*Magyar Tartalomszolgátatók Egyesülete (MTE) en Index.hu Zrt/Hongarije*).
58 EHRM 16 juni 2015, 64569/09, par. 144 (*Delfi/Estland*). Zie Klos 2022 (*supra* noot 25), p. 150-155.
59 EHRM 16 juni 2015, 64569/09, par. 113 (*Delfi/Estland*). Zie ook Par. 7 van Committee of Ministers, 'Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media', *Council of Europe*, 21 september 2011, beschikbaar op https://edoc.coe.int/en/media/8019-recommendation-cmrec20117-on-a-new-notion-of-media.html, p. 7-8.
60 Zie over deze verdeling van aansprakelijkheid R. Perry & T.Z. Zarsky, 'Who Should Be Liable for Online Anonymous Defamation?', *University of Chicago Law Review Dialogue* (82) 2015.
61 EHRM 16 juni 2015, 64569/09, par. 147 (*Delfi/Estland*).

en het karakter van de inhoud (hoe duidelijk herkenbaar en schadelijk?) een lijn die ook in de digitaledienstenverordening terug te vinden is.

3.3 Internetexceptionalisme in de digitaledienstenverordening

Zoals opgemerkt is de Richtlijn uit 2000 een stukje exceptionele wetgeving. In tegenstelling tot offlinediensten werd de aansprakelijkheid van zogenaamde hostingdiensten (diensten die op verzoek van gebruikers informatie opslaan) beperkt op voorwaarde dat 1) de aanbieder geen kennis had van de illegale inhoud en 2) indien de aanbieder kennis krijgt van de illegale inhoud deze prompt handelt en de informatie verwijdert of ontoegankelijk maakt.

De digitaledienstenverordening behoudt deze 'riante' uitzondering voor aansprakelijkheid voor inhoud aangeboden door derden. Zoals opgemerkt complementeert de digitaledienstenverordening dit met een systeem van publiek toezicht op basis van zorgvuldigheidsnormen. Een schending van deze zorgvuldigheidsnormen resulteert niet in aansprakelijkheid voor de inhoud geplaatst door derden, maar wordt publiekrechtelijk geadresseerd. In het meest bijzondere geval kan de digitaledienstencoördinator van een lidstaat[62] op basis van nationale wetgeving boetes opleggen van 'maximaal 6 % […] van de wereldwijde omzet van de betrokken aanbieder […] in het voorgaande boekjaar'.[63] Voor zeer grote onlineplatforms (of zoekmachines) met meer dan 45 miljoen actieve gebruikers per maand en die als zodanig zijn aanwezen door de Europese Commissie, kan de Europese Commissie zelf een onderzoek starten.[64]

In december 2023 startte de Europese Commissie een onderzoek. De digitaledienstenverordening was al eerder dan 17 februari 2024 van toepassing op zeer grote onlineplatforms.[65] De Europese Commissie heeft voor deze zeer grote onlineplatforms zelf mogelijkheden die zien op het doen van onderzoek,[66] het nemen van voorlopige maatregelen,[67] of bij niet-naleving te sanctioneren.[68] Ook hier gaat het om boetes van maximaal zes procent van de totale wereldwijde jaaromzet in het voorgaande boekjaar.[69] In het geval van een inbreuk op informatieverplichtingen gaat het doorgaans om maximaal één procent.[70]

De digitaledienstenverordening is hiermee exceptioneel op twee manieren. Allereerst geeft de digitaledienstenverordening in de relatie gebruiker/aanbieder de aanbieder een exceptionele positie: de aanbieder is (met goede redenen) niet direct aansprakelijk voor onrechtmatige inhoud, maar alleen na een voorafgaande melding én het niet prompt nemen van maatregelen na deze melding. Anders dan de traditionele redacties kunnen onlineplatforms niet worden verplicht om algemeen toezicht te houden op het platform. Het is ook moeilijk te zien hoe zulk toezicht

62 Voor Nederland wordt getuige de concept-uitvoeringswet de ACM aangewezen digitaledienstencoördinator (art. 2.2 van de Uitvoeringswet). Het wetvoorstel ligt op moment van schrijven (januari 2024) bij de Raad van State, zie Wetgevingskalender, 'Uitvoeringswet digitaledienstenverordening', *Overheid.nl*, beschikbaar op https://wetgevingskalender.overheid.nl/Regeling/WGK015094.
63 Art. 52 lid 3 Verordening (EU) 2022/2065.
64 Afdeling 4 van Hoofdstuk 5 Verordening (EU) 2022/2065.
65 Vergelijk art. 92 en 93 lid 2 Verordening (EU) 2022/2065.
66 Art. 67 tot 69 Verordening (EU) 2022/2065.
67 Art. 70 tot 72 Verordening (EU) 2022/2065.
68 Art. 73 en 74 Verordening (EU) 2022/2065.
69 Art. 74 lid 1 Verordening (EU) 2022/2065.
70 Art. 74 lid 2 Verordening (EU) 2022/2065.

eruit zou komen te zien: handmatig elke post controleren op onrechtmatige inhoud?[71] De digitaledienstenverordening neemt daarmee het hart van de exceptionele benadering uit 2000 over.

Tegelijkertijd is de digitaledienstenverordening exceptioneel, gelet op de behandeling van zeer grote onlineplatforms. Deze platforms hebben onder de digitaledienstenverordening aanvullende verplichtingen gekregen die kleinere diensten niet hebben gekregen. De digitaledienstenverordening stapelt verschillende exceptionele benaderingen: er wordt onderscheid gemaakt tussen online dienstverleners en offline dienstverleners, vervolgens wordt er onderscheid gemaakt tussen verschillende soorten diensten en daarnaast ook tussen hosting diensten die onlineplatformfunctionaliteiten aanbieden en diensten die dit niet doen. Daarbovenop wordt nog onderscheid gemaakt tussen zeer grote onlineplatforms en kleinere onlineplatforms.

Deze meer geraffineerde vorm van internetexceptionalisme is uiteraard niet over de volle breedte voordelig voor onlineplatforms. Het tegendeel is ook zeker niet waar: de *safe harbour* uit de Richtlijn blijft immers intact. Het internetexceptionalistische karakter van de digitaledienstenverordening laat zich niet kenmerken als 'utopisch' of 'paranoïde'. De derde golf van internetexceptionalisme zoals Goldman deze identificeerde in 2010, proliferatie van internetexceptionalisme, is ook nu nog springlevend.[72] De verplichtingen van onlineplatforms worden verder gedifferentieerd.

4 Exceptionalisme in de online aanpak?

Kenmerkend aan deze proliferatie van exceptionele wetgeving is dat wetgevers fijnmaziger te werk gaan door specifieke wetgeving te maken voor hele specifieke functionaliteiten.[73] De digitaledienstenverordening is hiervan een voorbeeld: specifieke risico's gecreëerd door bepaalde platformfunctionaliteiten worden geadresseerd met wetgeving die alleen van toepassing is op de mate waarin het risico zich op een platform kan verwezenlijken.[74] Een platform zonder videofunctionaliteiten zal bijvoorbeeld niet te maken krijgen met gemanipuleerde video's.

Tegelijkertijd is ook een andere beweging te zien. De wetgever in Nederland kiest er bijvoorbeeld voor niet onlineplatforms, maar gebruikers tot normadressant te maken. Het gaat hierbij om bijvoorbeeld strafwetgeving die niet alleen ziet op gedrag dat op het internet kan worden vertoond, maar ook van toepassing kan zijn op gedrag op straat.

Om deze twee tegengestelde bewegingen inzichtelijk te maken bespreek ik twee voorbeelden. Het gaat hierbij om twee relatief oude fenomenen die recentelijk een hernieuwde aanpak hebben gekregen. Het eerste voorbeeld is *doxing* (in de volksmond: openbaarmaking van persoonsgegevens met als doel intimideren) dat sinds 1 januari 2024 strafbaar is gesteld in Nederland. Dit betekent dat zowel gebruikers als (uiteindelijk) onlineplatforms aangesproken kunnen worden op dergelijke inhoud. Het tweede voorbeeld heeft een andere aanpak gekregen: desinformatie. Desinformatie wordt gereguleerd door middel van een gedragscode (de *Code of Practice on*

71 Zoals de beheerder van de Nederlandstalige 'porntubewebsite' vagina.nl deed, zie Rb. Amsterdam 16 februari 2022, ECLI:NL:RBAMS:2022:557, r.o. 5.9, *Computerrecht* 2022/96, m.nt. B.B.E. van der Donk & M. Klos (*Vagina.nl*).
72 Goldman 2010 (*supra* noot 5) p. 166-167. Zie ook Klos 2022 (*supra* noot 25), p. 36.
73 Goldman 2010 (*supra* noot 5) p. 166-167.
74 Art. 34 en 35 Verordening (EU) 2022/2065.

Disinformation) die, zoals zal worden besproken, sinds de digitaledienstenverordening onder omstandigheden ook verplicht kan worden gesteld.[75] Anders dan voor *doxing* kunnen gebruikers en onlineplatforms dus in beginsel niet strafrechtelijk aangesproken worden op desinformatie – tenzij er toevallig ook overlap is met stafbare inhoud.

4.1 *Doxing* op de straat?

Sinds 1 januari 2024 kent het Nederlands Wetboek van Strafrecht met artikel 285d lid 1 Sr een bepaling die *doxing* strafbaar stelt. *Doxing* wordt in met maximaal twee jaar celstraf of een geldboete van de vierde categorie bedreigd. Het gaat hierbij volgens de delictsomschrijving om iemand die

> 'zich persoonsgegevens van een ander of derden verschaft, deze gegevens verspreidt of anderszins ter beschikking stelt met het oogmerk om die ander vrees aan te jagen dan wel aan te laten jagen, ernstige overlast aan te doen dan wel aan te laten doen of hem in de uitoefening van zijn ambt of beroep ernstig te hinderen dan wel ernstig te laten hinderen.'[76]

De maximale celstraf kan met een derde verhoogd worden als het gaat om persoonsgegevens van

> 'een persoon in diens hoedanigheid van Minister, Staatssecretaris, commissaris van de Koning, gedeputeerde, burgemeester, wethouder, lid van een algemeen vertegenwoordigend orgaan, rechterlijk ambtenaar, advocaat, journalist of publicist in het kader van nieuwsgaring, ambtenaar van politie of buitengewoon opsporingsambtenaar.'[77]

Doxing wordt niet expliciet genoemd in de delictsomschrijving. Gelet op de delictsomschrijving kan een '*doxing* delict' ook gepleegd worden buiten het internet om. Wel is het van belang om op te merken dat het fenomeen en de terminologie een oorsprong heeft op het internet. Zo refereren *Urban Dictionary* en Wikipedia naar *doxing* als een internetfenomeen.[78] Ook de *Cambridge Dictionary* koppelt *doxing* expliciet aan het internet.[79]

Ook uit de overheidscommunicatie wordt duidelijk dat het om een internetfenomeen gaat. De Rijksoverheid definieert *doxing* (overeenkomstig de wet) als het delen van persoonsgegevens met het doel om te intimideren. Wel refereert de Rijksoverheid aan de impact voor slachtoffers als persoonsgegevens op internet blijven staan. Ook verwijst de Rijksoverheid door naar Helpwanted.nl (gespecialiseerd in hulp bij online grensoverschrijdend gedrag). Ook de Rijksoverheid

75 European Commission, '2022 Strengthened Code of Practice on Disinformation', *European Commission*, 21 juli 2022, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.
76 Art. 285d lid 1 Sr.
77 Art. 285d lid 2 Sr.
78 Urban Dictionary, 'doxing', *Urban Dictionary*, beschikbaar op https://urbandictionary.com/define.php?term=doxing; Wikipedia, 'Doxing', *Wikipedia*, 12 januari 2024, beschikbaar op https://en.wikipedia.org/wiki/Doxing.
79 Cambridge Dictionary, 'doxing', *Cambridge Dictionary*, beschikbaar op https://dictionary.cambridge.org/dictionary/english/doxing.

heeft het online karakter van *doxing* dus op het oog.[80] In een weblog van het Ministerie van Justitie en Veiligheid komt nog duidelijker naar voren dat de achtergrond ligt in de toename van online intimidatie.[81] Ook de vraag en antwoordpagina van de Rijksoverheid is toegesneden op het internet.[82]

Uiteraard heeft het internet het plegen van bepaalde feiten makkelijker gemaakt (neem bijvoorbeeld het inbreuk maken op auteursrechten). Ook heeft het internet nieuw gedrag mogelijk gemaakt waarvoor een strafbaarstelling noodzakelijk was (computervredebreuk). Bovendien zijn er strafbare feiten waarvan het bereik, en dus ook het mogelijke effect, groter is als het een online dimensie krijgt (opruiing). Daarnaast kunnen uitingsdelicten langer effect hebben op het internet. Het internet vergeet immers niet (of slechts heel moeilijk) en het verdelen delen van strafbare inhoud (wat weliswaar ook strafbaar kan zijn) is erg eenvoudig. Bij *doxing* gaat het echter om een fenomeen dat een sterke online oorsprong kent, maar nu ook een offline strafbaarstelling kent. Het lijkt hier om een omgekeerde 'wat offline niet mag, kan ook online niet' te gaan.

De vraag is echt of de wetgever offline gedragingen op het oog had bij deze strafbaarstelling. Buiten het bekladden van toiletvoorzieningen met bijvoorbeeld het 06-nummer van de te doxen persoon is het moeilijk voor te stellen hoe *doxing* slechts een 'zuiver' offline dimensie kan hebben. Weliswaar is de strafbaarstelling in artikel 258d Sr niet beperkt tot *doxing* in het openbaar. Het is echter moeilijk voor te stellen dat er opsporing wordt gestart voor enkel en alleen *doxing* zonder dat dit het geval is.

4.2 Desinformatie als platformprobleem

De aanpak van desinformatie verschilt van de aanpak van *doxing* doordat de aanpak hiervan ook juridisch specifiek is gericht op het internet. In het geval van *doxing* kan het normenkader offline ook van toepassing zijn, bij desinformatie is dit niet het geval. Indien desinformatie wordt verspreid in een huis-aan-huisblad wordt dit anders gereguleerd dan desinformatie op onlineplatforms. Voor de digitaledienstenverordening ging het om in beginsel niet-afdwingbare verplichtingen neergelegd in vrijwillige gedragscodes.[83] Na de digitaledienstenverordening is er sprake van een co-reguleringssysteem als het gaat om zeer grote onlineplatforms waarin gedragscodes een grote rol spelen.[84] Zeer grote onlineplatforms kunnen door de Europese Commissie worden gevraagd deel te nemen aan een gedragscode om een inbreuk op de verplichtingen uit de

80 Rijksoverheid, 'Doxing', *Rijksoverheid*, beschikbaar op https://rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/doxing.

81 Ministerie van Justitie en Veiligheid, 'Nieuwe wet tegen doxing "Je staat er niet alleen voor!"', *Rijksoverheid*, 2 januari 2024, beschikbaar op https://rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/het-verhaal-van-j-en-v/2024/nieuwe-wet-tegen-doxing-je-staat-er-niet-alleen-voor.

82 Rijksoverheid, 'Wat kan ik doen als ik slachtoffer ben van doxing?', *Rijksoverheid*, beschikbaar op https://rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/wat-kan-ik-doen-als-ik-slachtoffer-ben-van-doxing.

83 European Commission, 'Code of Practice on Disinformation', *European Commission*, 2018, beschikbaar op https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation; European Commission, '2022 Strengthened Code of Practice on Disinformation', *European Commission*, 21 juli 2022, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

84 Overwegingen 88, 89, 92-93 99, 103-106 en 150 Verordening (EU) 2022/2065.

digitaledienstenverordening te voorkomen.[85] De naleving van de gedragscode is daarna niet meer vrijwillig, maar onderdeel van het handhavingssysteem van de digitaledienstenverordening.[86]

Het in eerste instantie geheel vrijwillige karakter van desinformatieregulering en de uitwerking van regulering in gedragscodes laat het bijzondere en complexe karakter van desinformatie zien. Immers zijn er grote zorgen over de proliferatie van desinformatie, maar dit gaat ook op voor de impact van desinformatieregulering op de vrijheid van meningsuiting. Dit wordt veroorzaakt door het karakter van desinformatie.

Allereerst is het probleem dat desinformatie zich niet makkelijk laat definiëren. Desinformatie kent slechts een (zeer) beperkte juridische afbakening. Net als bij *doxing* komt het woord desinformatie dan ook niet letterlijk voor in de wetboeken. Anders dan bij *doxing* is er echter geen juridische omschrijving die aansluit bij het concept desinformatie opgenomen. Zelfs de digitaledienstenverordening maakt in de artikelen geen melding van desinformatie.
De definities die worden gebruikt voor desinformatie zijn voornamelijk academisch van aard[87] of meer bedoeld als beleidsdefinitie.[88] De juridische betekenis van desinformatiedefinities is dus gering als het gaat om het reguleren van door gebruikers geplaatste inhoud. Bepalend is voornamelijk hoe aanbieders van onlineplatforms desinformatie adresseren in hun gebruikersvoorwaarden.[89] Om een breder begrip te krijgen van het concept desinformatie worden hier wel de elementen besproken die terugkomen in de definitie van de Europese Commissie. Veel van deze elementen komen ook terug in andere definities – met uiteraard wel wat accentverschillen.

De Europese Commissie definieert desinformatie in de *Code of Practice* uit 2018 als 'verifiably false or misleading information' die cumulatief (1) '[i]s created, presented and disseminated for economic gain or to intentionally deceive the public' en (2) '[m]ay cause public harm' wat in ieder geval bedreigingen voor het democratisch proces omvat maar ook de gezondheid van EU-burgers, het milieu of de veiligheid.[90] In 2022 is in de *Strenghtened Code of Practice* desinformatie gelijk komen te vallen met onder andere misinformatie.[91] Hiermee is de opzettelijke verspreiding van verifieerbare valse of misleidende informatie gelijk komen te vallen met de onopzettelijke variant.

Het is verleidelijk om desinformatie te vergelijken met uitingsdelicten zoals wij deze kennen in het Wetboek voor Strafrecht. Hoewel opzettelijk onjuiste claims over personen verspreiden

85 Art. 45 lid 2 Verordening (EU) 2022/2065.
86 Art. 45 lid 4 Verordening (EU) 2022/2065.
87 Zie voor een overzicht R. Ó Fathaigh, N. Helberger & N. Appelman, 'The perils of legally defining disinformation', *Internet Policy Review* (10) 2021, afl. 4, doi:10.14763/2021.4.1584.
88 European Commission, 'Code of Practice on Disinformation', *European Commission*, 2018, beschikbaar op https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation; European Commission, '2022 Strengthened Code of Practice on Disinformation', *European Commission*, 21 juli 2022, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.
89 Art. 14 Verordening (EU) 2022/2065.
90 European Commission, 'Code of Practice on Disinformation', *European Commission*, 2018, beschikbaar op https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.
91 European Commission, '2022 Strengthened Code of Practice on Disinformation', *European Commission*, 21 juli 2022, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation, p. 1.

(laster)[92] of de opruiing tot een strafbaar feit onder omstandigheden kunnen overlappen met (de vaak weinig strak omlijnde) definities van desinformatie, is inhoud die wordt gereguleerd als desinformatie veel breder.

Zoals opgemerkt is desinformatie gelijkgesteld met misinformatie in de praktijkcode uit 2022.[93] Deze gelijkstelling is gelet op de praktijkcode niet noodzakelijk problematisch. Het gaat immers in het geval van de praktijkcode niet automatisch om het verwijderen van inhoud als desinformatie, maar om een waaier van maatregelen waaronder het beperken van de zichtbaarheid, het aanbevelen van inhoud in de zoekresultaten of in de tijdlijn van gebruikers of het plaatsen van waarschuwingen of het bieden van extra context.[94] Als wordt overgegaan tot een strafbaarstelling moet er sprake van zijn van een zekere mate van verwijtbaarheid. Daarbij is het lastig om vast te stellen of het inderdaad desinformatie betreft of de niet-opzettelijke variant misinformatie. Dit kan leiden tot een overinclusieve of juist een te beperkte bepaling.[95] Zeker als burgers de bepaling zwaar oppakken kan dit leiden tot zelfcensuur (een '*chilling effect*') waarbij ook legale uitingen die niet beoogd worden door de regulering uit vrees voor mogelijke strafbaarheid achterwegen gelaten worden.[96] Ditzelfde effect kan mogelijk optreden op onlineplatforms als zij overgaan tot overmoderatie van inhoud die niet noodzakelijk illegaal is. Bijvoorbeeld omdat onlineplatforms moeilijk toepasbare juridische definities moeten handhaven.[97]

Hetzelfde geldt voor het vaststellen of er sprake is van verifieerbare valse of misleidende informatie. Dit is voor leken van een betreffend kennisgebied niet altijd makkelijk te bepalen. Zeker in situaties waarin desinformatieregulering nuttig zou zijn is de kans aanwezig dat er veel onzeker/onduidelijk is waardoor het ook lastig is om vast te stellen of iets misleidend of onjuist is.[98]

Het reguleren van desinformatie in de strafwet kan in potentie een grote impact hebben op de uitingsvrijheid. De keuze voor een praktijkcode gericht aan onlineplatforms weet dit deels te voorkomen. Niet de overheid bepaalt wat exact te gelden heeft als desinformatie en wat niet, maar private onlineplatforms. Deze dienen in hun gebruiksvoorwaarden op te nemen wat zij verstaan onder desinformatie en welke remedies zij kunnen toepassen indien zij inhoud modereren dat kwalificeert als desinformatie.[99] Hierbij dienen onlineplatforms volgens de digitaledien-

92 Art. 262 lid 1 Sr.

93 European Commission, '2022 Strengthened Code of Practice on Disinformation', *European Commission*, 21 juli 2022, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

94 European Commission, 'Code of Practice on Disinformation', *European Commission*, 2018, beschikbaar op https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation. European Commission, '2022 Strengthened Code of Practice on Disinformation', *European Commission*, 21 juli 2022, beschikbaar op https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

95 Zie ook I. Siegel & M. Klos, 'Straffe desinformatiewetgeving? Bedenkingen vanuit Franse en Europese Uniewetgeving', *Ars Aequi* 2024, 7/8, p. 689-691.

96 F. Schauer, 'Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"', *Boston University Law Review* (58) 1978, afl. 5, p. 693.

97 Dit is geen theoretisch probleem, zie D. Keller, 'Empirical Evidence of "Over-Removal" by Internet Companies Under Intermediary Liability Laws', *The Center for Internet and Society*, 8 februari 2021, beschikbaar op https://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.

98 Zie ook Siegel & Klos 2024 (*supra* noot 95), p. 689-691.

99 Art. 14 lid 1 Verordening (EU) 2022/2065.

stenverordening rekening te houden met de rechten van gebruikers – waaronder het recht op vrijheid van meningsuiting.[100]

Omdat de Europese Commissie vooral de online verspreiding van desinformatie als uitgangspunt neemt is deze exceptionele online aanpak te verklaren.[101] Desinformatie is online gelet op de snelle, grootschalige verspreiding een groter probleem dan offline varianten. Tegelijkertijd kunnen online minder ingrijpende oplossingen genomen worden dan bij offline media het geval is. Goldman merkt op dat het mogelijk is om online remedies te programmeren die offline nooit mogelijk zouden zijn.[102] Denk hierbij bijvoorbeeld aan remedies die worden gebruikt in computerspelletjes waarbij de digitale avatar van een valsspeler onzichtbaar wordt gemaakt en niet kan interacteren met andere spelers.

Tegelijkertijd moet de mogelijke impact op de online uitingsrechten van gebruikers niet onderschat worden. Zeker als onlineplatforms overgaat tot het verwijderen als inhoud omdat het desinformatie zou betreffen. Omdat onlineplatforms mogen modereren overeenkomstig hun eigen gebruikersvoorwaarden is het de vraag of klagen bij het platform zelf een gewenst effect heeft.[103] Het werken met gedragscodes en afspraken tussen de Europese Commissie en onlineplatforms wordt door Amerikaanse commentatoren zoals Danielle Citron als buitenrechtstatelijke overheidsdwang gezien.[104] Normen die vaak ook buiten de EU effect sorteren.[105]

5 Conclusie

Wat offline niet kan, kan ook online niet. Voor het beschermen van de privacyrechten van gebruikers is dit zonder meer een niet meer dan logisch uitgangspunt. Als dit gerelateerd wordt aan de uitingsrechten van gebruikers ontstaat een ander beeld. Het internet biedt mensen een kans om een enorm publiek te bereiken. Dit betekent ook dat schadelijke inhoud online grotere gevolgen kan hebben. Dit heeft enerzijds te maken met de schaal, anderzijds met het persistente karakter van online inhoud.

Dit maakt dat het online en offline inhoud wel degelijk anders wordt gereguleerd. De Nederlandse wetgever heeft met het aanpakken van *doxing* voornamelijk online inhoud op het oog – ook al wordt ook offline *doxing* gecriminaliseerd. Bij de aanpak van desinformatie wordt er in tegenstelling tot *doxing* duidelijk gedifferentieerd tussen online en offline inhoud. Deels valt dit te verklaren vanuit het juridisch slecht omlijnde karakter van desinformatie: het is niet eenvoudig passende offlinemaatregelen te nemen. Terwijl op internet de zichtbaarheid beperkt kan worden, context kan worden geboden of andere maatregelen genomen kunnen worden is dit voor offline uitingen veel ingrijpender. Anderzijds is het probleem online ook groter: juist de verdere verspreiding van desinformatie wordt tegengegaan.

100 Art. 14 lid 4 Verordening (EU) 2022/2065. Siegel & Klos 2024 (*supra* noot 95), p. 686.
101 Communication COM(2018)236 final van the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions van 26 april 2018 Tackling Online Disinformation: A European Approach, p. 5-6.
102 Goldman 2021 (*supra* noot 6) p. 11. Siegel & Klos 2024 (*supra* noot 95), p. 686.
103 Art. 14 jo. 20 Verordening (EU) 2022/2065.
104 D. Citron, 'Extremist Speech, Compelled Conformity, and Censorship Creep', *Notre Dame Law Review* (93) 2018, afl. 3, p. 1070.
105 A. Bradford, 'The Brussels Effect', *Northwestern University Law Review* (107) 2012, afl. 1, p. 6.

Hoewel de digitaledienstenverordening beoogt de verantwoordelijkheid van internettussenpersonen verder te expliciteren en meer in overeenstemming te brengen met de mogelijke controle die onlineplatforms kunnen uitoefenen, kan de digitaledienstenverordening ook worden gezien als een bevestiging van een internetexceptionalitistische benadering. De digitaledienstenverordening uit 2022 kent zelfs exceptionele regels voor verschillende soorten aanbieders van digitale diensten. Veel van deze regels bestaan uit zorgvuldigheidsverplichtingen die nader worden ingekleurd na bijvoorbeeld een risicobeoordeling (volgens artikel 34 van de digitaledienstenverordening). Weliswaar geeft artikel 35 van de digitaledienstenverordening een lijst van mogelijke aandachtspunten waarmee deze risico's beperkt kunnen worden, dit geeft niet aan in welke mate dit dient te worden gedaan en hoe deze beperkingen er dan uit dienen te zien.

Het risico bestaat dat door deze benadering dat online inhoud inderdaad exceptioneel wordt benaderd in de zin dat bestaande kader die de vrijheid van meningsuiting van gebruikers dienen te waarborgen door het gebruik van gedragscodes niet (volledig) worden toegepast. Daarmee verliest deze benadering juist een belangrijk voordeel. Doordat desinformatie niet illegaal is kan een fijnmaziger systeem van remedies worden toegepast waarbij ook de vrijheid van meningsuiting expliciet wordt meegewogen.

Dat brengt mij tot een afsluiting. Expliciet internetexceptionalisme kan juist bijdragen aan een betere weging van de verschillende rechten. Het gelijkstellen van verboden voor zowel de online en offlinewereld kan als ongewenst effect hebben dat een fijnmazig systeem van inhoudsregulering vervangen wordt tot een juridische plicht tot verwijdering. Ook onder de digitaledienstenverordening kan een hostingdienst dat wordt geconfronteerd met illegale inhoud niets anders dan het verwijderen van deze inhoud, omdat de dienst zich anders blootstelt aan aansprakelijkheid voor deze inhoud.