

De Digital Services Act na één jaar: naar een meer betrouwbare onlineomgeving?

Computerrecht 2025/46

In 2024 introduceerde de Digital Services Act (DSA) een uitgebreide reeks wettelijke verplichtingen die gericht zijn op het bevorderen van een meer veilige en betrouwbare onlineomgeving binnen de EU. Een jaar na de inwerkingtreding van de verordening hebben zich verschillende interessante ontwikkelingen voorgedaan wat betreft het aanbieden van tussenhandeldiensten. Van aanwijzingsbesluiten gepubliceerd door de Europese Commissie tot de vrijgave van onafhankelijke auditrapporten over zeer grote onlineplatforms en onlinezoekmachines: een kritische analyse van de recente ontwikkelingen biedt waardevolle inzichten in de praktische toepassing van de DSA, alsook in de uitdagingen die gepaard gaan met de handhaving van de verordening. Deze bijdrage beoogt enerzijds om de belangrijkste nieuwe inzichten over de DSA samen te brengen, en anderzijds om nieuwe spanningen in kaart te brengen. Daarbij gaat bijzondere aandacht uit naar contentmoderatie en de verplichting tot algoritmische transparantie.

1. Inleiding

De geleidelijke opmars van microchips en informatietechnologie heeft een ware revolutie teweeggebracht wat betreft de manier waarop we met elkaar communiceren, informatie verwerken, aankopen doen en – meer algemeen – hoe we ons leven leiden. De explosieve toename aan digitale activiteit ging op zijn beurt gepaard met de opkomst van talrijke onlineplatforms, die anno 2025 onze digitale omgeving voor een groot deel vormgeven. Van sociale mediasites tot appstores en e-commerce websites: het zijn platforms waar we quasi op dagelijkse basis mee interageren. Enerzijds stellen dergelijke platforms ons in staat om veel facetten van ons dagelijks leven te regelen vanuit het comfort van onze woning. Anderzijds brengen ze ook markante nieuwe juridische vraagstukken met zich mee, bijvoorbeeld wat betreft de aansprakelijkheid voor illegale inhoud of de moderatie van dergelijke platformomgevingen.³

Als reactie hierop heeft de Europese Commissie (EC) in 2020 haar visie uiteengezet voor de verdere regulering van het digitale landschap. Via de mededeling “*Shaping Europe's digital future*”⁴ verduidelijkt de EC dat het verder uitbouwen van digitale technologie dient plaats te vinden op basis van een Europees waardenkader, waarbij vooral de EU-burger centraal staat.⁵ Die visie kreeg in datzelfde jaar een meer concrete vorm onder de noemer van een “*Digital Services Act package*”,⁶ waarbinnen twee wetgevende voorstellen werden gelanceerd. Ten eerste gaat het over de Digitaalemarktenverordening⁷ (*Digital Markets Act*; DMA), die de EU in staat stelt om ondernemingen aan te duiden als poortwachters, waardoor verschillende verplichtingen van toepassing worden om een meer competitieve digitale markt te creëren. Ten tweede gaat het over de Digitaal dienstenverordening⁸ (*Digital Services Act*; DSA). Binnen het bestek van deze bijdrage ligt de focus bij dit laatste instrument.

Een inhoudelijke beschouwing van de DSA leert ons dat de verordening een ambitieuze set aan regels omvat die onder meer eerdere EU-wetgeving m.b.t. digitale diensten moderniseert.⁹ Voorname speerpunten van de DSA zijn bijvoorbeeld het introduceren van nieuwe verplichtingen voor het verwijderen van illegale inhoud, het opleggen van transparantieplichtingen voor online advertenties, en het invoeren van risicobeoordelingen voor zeer grote onlineplatforms (*Very Large Online Platforms*; VLOP's) en zeer grote onlinezoekmachines (*Very Large Online Search Engines*; VLOSE's). Aan de hand van dit gemoderniseerd regime engageert de DSA zich om bij te dragen aan een meer veilige, voorspelbare, en vooral ook betrouwbare onlineomgeving waar in de eerste plaats de rechten van gebruikers worden gewaarborgd, maar waar er tegelijkertijd ook aandacht is voor het stimuleren van innovatie en economische groei.¹⁰

1 Christof Koolen werkt als postdoctoraal onderzoeker bij het Centrum voor IT- en IP-recht (CITIP) van de KU Leuven.
E-mail: christof.koolen@kuleuven.be.

2 Monica Schellemans is doctoranda bij het Instituut voor Consument, Concurrentie & Markt (CCM) van de KU Leuven.
E-mail: monica.schellemans@kuleuven.be.

3 Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende een eengemaakte markt voor digitale diensten [2020] COM(2020) 825 final 2.

4 Communicatie van de Commissie – De digitale toekomst van Europa vormgeven [2020] COM(2020) 67 final.

5 *Ibid.* 2-3.

6 Europese Commissie, ‘The Digital Services Act Package’ (*Europese Commissie*, 4 oktober 2024) <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>> geraadpleegd op 5 december 2024.

7 Verordening (EU) 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector (digitaalemarktenverordening).

8 Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten (digitaal dienstenverordening).

9 De eerste stappen voor de regulering van digitale diensten waren genomen in 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’).

10 Rechtsoverweging 4, DSA.

Verschillende spraakmakende mediaberichten – bijvoorbeeld omtrent sociaalnetwerksite X¹¹ – tonen aan dat de DSA een significante weerslag heeft op het verstrekken van zogenaamde tussenhandeldiensten (*intermediary services*). Hieruit valt reeds op te maken dat, hoewel de DSA een belangrijke stap neemt in de richting van een coherente en gecoördineerde aanpak voor het verlenen van digitale diensten, er ook prominente vraagstukken opduiken omtrent het vinden van een evenwicht tussen verschillende rechten en belangen. Een passend voorbeeld hiervan is het spanningsveld tussen contentmoderatie en het recht op vrijheid van meningsuiting.

In het licht hiervan gaan we in dit artikel na hoe de DSA onze onlineomgeving beïnvloedt en werpen we, waar nodig, kritische vragen op. Met die doelstelling in het achterhoofd biedt deze bijdrage een diepgaande analyse van de DSA, waarbij er voorname aandacht uitgaat naar recente ontwikkelingen sinds de inwerkingtreding van de verordening op 17 februari 2024. De structuur van dit artikel is vijfledig. Na deze inleidende sectie behandelt *Sectie 2* de doelstellingen, het toepassingsgebied, en de inhoudelijke verplichtingen van de DSA. Vervolgens gaat *Sectie 3* in op de verschillende processen voor contentmoderatie en het verwijderen van illegale inhoud. Daarna bespreekt *Sectie 4* de verplichting tot algoritmische transparantie binnen de DSA. Tot slot biedt *Sectie 5* een aantal overkoepelende beschouwingen.

2. Het juridisch kader van de DSA ontleed

2.1 Context

Het is vooreerst relevant om aan te stippen dat de DSA beoogt om een overkoepelend regime aan te bieden voor het verlenen van diensten in de onlineomgeving. Binnen dit regime gaat er bijzondere aandacht uit naar een nieuw aansprakelijkheidsregime¹² en inhoudelijke zorgvuldigheidsverplichtingen.¹³ Een analyse van de rechtsoverwegingen van de DSA leert ons dat de verordening zich verankert aan het begrip ‘tussenhandeldienst’. Bij dergelijke tussenhandeldiensten zijn er vervolgens twee facetten die de aandacht verdienen: enerzijds maken dergelijke diensten het voor gebruikers mogelijk om online informatie te raadplegen en transacties af te sluiten, anderzijds kunnen gebruikers tussenhandeldiensten ook aanwenden voor het verspreiden van illegale inhoud en desinformatie^{14,15}

Vermits uiteenlopende nationale regimes dergelijke risico's trachten te ondervangen, stelt de DSA een geharmoniseerde, Europese aanpak voorop om verdere versnippering binnen de platformregulering te voorkomen.¹⁶ Finaal heeft deze harmonisatieaanpak één duidelijk afgebakende doelstelling: het waarborgen van een veilige, voorspelbare, en betrouwbare onlineomgeving.¹⁷

2.2 Aanknopingspunten

De structuur van de DSA is relatief complex en kan aanleiding geven tot de nodige terminologische verwarring. In het licht daarvan is het nuttig om het schematisch overzicht op p. 88 voor ogen te houden.

2.2.1 Diensten van de informatiemaatschappij

Uit het schema volgt dat het begrip ‘dienst van de informatiemaatschappij’ (*information society service*) een zeer breed scala aan digitale diensten beslaat,¹⁸ waarvan een specifiek segment vervolgens ook kan kwalificeren als een tussenhandeldienst. Beide begrippen overlappen bijgevolg niet volledig. Ter herinnering: de EU-wetgever hanteert vijf cumulatieve criteria als maatstaf voor de kwalificatie van een dienst als een dienst van de informatiemaatschappij:¹⁹

- (i) Een dienst;
- (ii) Gewoonlijk tegen vergoeding;
- (iii) Op afstand;
- (iv) Via elektronische weg.

Bijgevolg zal een onlinebankingapp in aanmerking komen als een dienst van de informatiemaatschappij (doch niet als een tussenhandeldienst, zoals verder toegelicht). Dezelfde redenering geldt ook voor e-commerceplatforms die zich toespitsen op directe detailhandel tegenover een eindgebruiker (bv. de webshop van Zara, H&M, of IKEA): ook hier is een kwalificatie als dienst van de informatiemaatschappij correct (doch niet als tussenhandeldienst, zoals verder toegelicht).

2.2.2 Tussenhandeldiensten

De volgende stap omvat logischerwijze het verder onderscheiden van de term ‘tussenhandeldienst’ tegenover het begrip ‘dienst van de informatiemaatschappij’. Een tus-

11 Supantha Mukherjee, ‘EU Targets Musk’s X in First Illegal Content Probe’ (*Reuters*, 18 december 2023) <<https://www.reuters.com/technology/eu-opens-proceedings-against-x-over-its-efforts-combat-information-manipulation-2023-12-18/>> geraadpleegd op 5 december 2024.

12 Artikel 4 *et seq.*, DSA.

13 Artikel 11 *et seq.*, DSA.

14 Over de invulling van het begrip ‘desinformatie’, zie Alain Strowel en Jean De Meyere, ‘The Digital Services Act: Transparency as an Efficient Tool to Curb the Spread of Disinformation on Online Platforms?’ (2023) 14 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 66, 68–70.

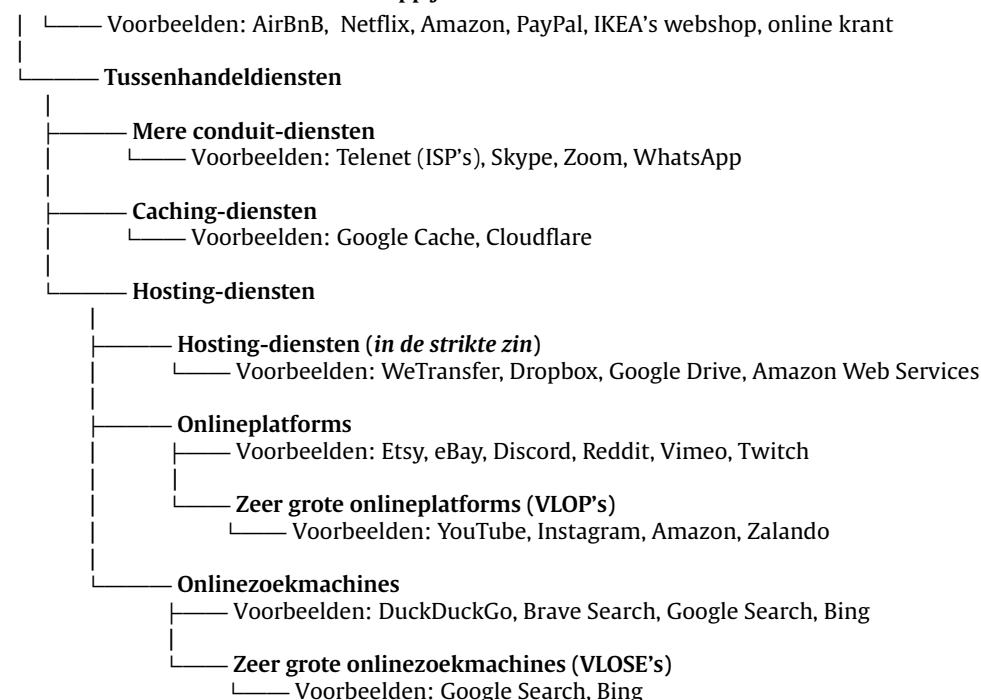
15 Rechtsoverwegingen 1–2, DSA.

16 Rechtsoverweging 2, DSA; Miriam C Buiten, ‘The Digital Services Act from Intermediary Liability to Platform Regulation’ (2021) 12 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 361, 365; Teresa Rodríguez de las Heras Ballell, ‘The Background of the Digital Services Act: Looking towards a Platform Economy’ (2021) 22 *ERA Forum* 75, 79–80.

17 Rechtsoverweging 3, DSA.

18 Voor een meer uitgebreide analyse, zie Maciej Szpunar, ‘Reconciling New Technologies with Existing EU Law – Online Platforms as Information Society Service Providers’ (2020) 27 *Maastricht Journal of European and Comparative Law* 399, 401.

19 Artikel 1, Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij; zie ook Zaak C-62/19, *Star Taxi App* [2020] ECLI:EU:C:2020:980, para 42; Caterina Gardiner, ‘Star Taxi App Is an “Information Society Service”: But Is the Meter Still Running for the Classification of Platform Services?’ (2021) 10 *Journal of European Consumer and Market Law* 67, 68.

Diensten van de informatiemaatschappij

senhandeldienst voldoet per definitie ook aan de vijf hogervermelde kenmerken van een dienst van de informatiemaatschappij. Anders gesteld: tussenhandeldiensten zijn een deelverzameling van de overkoepelende categorie van diensten van de informatiemaatschappij. Het specifieke onderscheid tussen deze twee categorieën ligt in het feit dat *tussenhandeldiensten zich specifiek richten op het doorgeven, opslaan, of toegankelijk maken van door gebruikers verstrekte informatie*.²⁰ Wat de verdere invulling hiervan betreft laat de DSA weinig ruimte voor interpretatie en gaat het over drie duidelijk afgebakende gevallen:²¹

- (i) *Mere conduit-diensten*:²² de Nederlandse vertaling van dit begrip geeft een goed beeld van de onderliggende dienst. Het gaat immers over een 'louter doorgeefluik' van informatie. De dienstverlener verricht m.a.w. een dienst die er enkel uit bestaat om informatie door te geven aan de afnemer van de dienst, zonder deze informatie aan te passen. Typevoorbeelden binnen deze categorie zijn zogenaamde Internet Service Providers (bv. Telenet, KPN), die gebruikers in staat stellen om de inhoud van websites te consulteren. Ook telecommunicatiediensten (bv. Skype, Zoom) en berichtenapps (bv. WhatsApp, Signal) vallen – in de regel²³ – onder deze hoofding vermits deze dienstverleners eveneens informatie van verzender tot ontvanger overdragen zonder aanpassingen aan de inhoud uit te voeren.

- (ii) *Caching-diensten*:²⁴ de term caching refereert aan het (tijdelijk) creëren en opslaan van een kopie van bepaalde gegevens, zodanig dat deze gegevens gemakkelijk toegankelijk blijven zonder de originele bron te moeten raadplegen. Het meest duidelijke voorbeeld in deze context is Google Cache, waarbij Google momentopnames vastlegt van websites zodanig dat gecachte webpagina's nog voor een tijdje toegankelijk blijven voor internetgebruikers, zelfs wanneer de oorspronkelijke website offline zou gaan. Een andere noemenswaardige dienstverlener in dit verband is Cloudflare, die bekendstaat voor zogenaamde *content delivery network* (CDN) caching, waarbij online inhoud (bv. foto's of video's van een website) wordt gedupliceerd en opgeslagen op meerdere aparte locaties (zgn. caching-servers). Op die manier kan de impact van surfende gebruikers worden verdeeld over de verschillende caching-servers en kan overbelasting van de oorspronkelijke bron worden vermeden.
- (iii) *Hosting-diensten*:²⁵ de kern van hosting-diensten omvat het opslaan van informatie die door gebruikers wordt verstrekt. Op die manier komen verschillende specifieke diensten in het vizier, zoals webhostingdiensten (waarbij de gebruiker een website, foto's of video's, of software kan bewaren), socialemediaplatforms (waarbij de gebruiker berichten kan posten), of onlinemarktplaatsen (waarbij de gebruiker advertenties kan plaatsen om voorwerpen te verkopen). Typisch voor hosting is bijgevolg het gegeven dat de dienstverlener webruimte ter beschikking stelt, die de gebruiker vervolgens meer concreet kan invullen. Een passend voorbeeld in deze

20 Voor een exemplarische opsomming van verschillende tussenhandeldiensten, zie rechtsoverweging 29, DSA.

21 Rechtsoverweging 5, DSA; artikel 3(g), DSA.

22 Artikel 3(g)(i), DSA.

23 Noteer echter de bedenkingen omtrent de kwalificatie van berichtenapp Telegram, zoals hieronder uiteengezet.

24 Artikel 3(g)(ii), DSA.

25 Artikel 3(g)(iii), DSA.

context is de stopzetting van de samenwerking tussen Amazon Web Services en het controversiële socialmediaplatform Parler in 2021: Amazon weigerde om haar servers ter beschikking te stellen aan Parler gelet op het feit dat leden de website gebruikten om haatdragende berichten te verspreiden en aan te zetten tot geweld.²⁶ In deze situatie wordt Amazon Web Services beschouwd als een hosting-dienst.

2.2.3 Onlineplatforms en onlinezoekmachines

2.2.3.1 Onlineplatforms

Zoals hoger gevisualiseerd, is het mogelijk om de categorie hosting-diensten verder uit te splitsen in enerzijds onlineplatforms, en anderzijds onlinezoekmachines. Kort samengevat moet een *onlineplatform* worden beschouwd als een hosting-dienst die niet alleen informatie opslaat, maar die deze informatie ook verder verspreidt onder het publiek.²⁷ Meer concreet impliceert dit dat de dienst instaat voor het delen van door gebruikers gegenereerde inhoud (*user-generated content*; UGC) of het faciliteren van de verdere verspreiding van dergelijke inhoud naar een groter publiek. Parler kwalificeert bijgevolg als een hosting-dienst die bovendien ook een onlineplatform uitmaakt, aangezien het boodschappen van haar gebruikers verspreidde onder een ruimer publiek. Amazon Web Services, daarentegen, is een hosting-dienst die geen onlineplatform is omdat de verleende dienst zich louter beperkt tot het ter beschikking stellen van webhosting servers.²⁸ Voor de kwalificatie als onlineplatform – waar meer verregaande inhoudelijke verplichtingen aan gekoppeld zijn – is het voorts nuttig om aan te stippen dat een hosting-dienst niet als onlineplatform in aanmerking komt wanneer de verspreiding van informatie slechts een bijkomstig element is van een andere, meer doorslaggevende dienst. In dit verband haalt de DSA zelf het voorbeeld aan van een commentaarsectie op de website van een krant.²⁹

Wat betreft de afbakening van onlineplatforms heerst er discussie over de exacte draagwijdte van het sleutelcriterium ‘verspreiden bij het publiek’.³⁰ Vooreerst: indien er geen verspreiding is van informatie van een gebruiker onder een ruimer publiek, volgt logischerwijs dat een kwalificatie als onlineplatform niet mogelijk is. De omgekeerde redenering gaat echter niet volledig op: niet elke vorm van verspreiding van informatie komt immers in aanmerking als een ‘verspreiding bij het publiek’ in de zin van artikel 3(k) DSA. Er is namelijk enkel sprake van een ver-

spreiding bij het publiek indien de informatie ter beschikking wordt gesteld “aan een potentieel onbeperkt aantal personen”.³¹

Enige bijkomende uitleg omtrent dit criterium is terug te vinden in rechtsoverweging 14. Hierin staat opgenomen dat, hoewel een eindgebruiker bepaalde informatie in eerste instantie online plaatst, er slechts sprake is van ‘verspreiding’ wanneer het platform de informatie gemakkelijk toegankelijk maakt voor andere leden van de platformomgeving, bijvoorbeeld door de info te laten verschijnen in een nieuwsfeed. Hier hangt echter ook aan vast dat informatie enkel kan worden beschouwd als ‘verspreid bij een publiek’ indien het verkrijgen van toegang tot de informatie automatisch gebeurt – of alleszins zonder een menselijke beslissing – zoals dat het geval is voor een video gepost op YouTube, een livestream gehost via Twitch, of een bericht geplaatst in een (publieke) Discord-community. In al deze gevallen is de informatie vrij toegankelijk voor het ruimere publiek, al dan niet mits het creëren van een account op het desbetreffende platform. Dezelfde redenering gaat echter niet op voor situaties waarbij inhoud wordt geplaatst in afgeschermd community’s of groepsgesprekken, waarbij ofwel de toegang tot de informatie wordt bepaald door een beheerder, ofwel de verspreiding van de informatie beperkt blijft tot een “bepaald eindig aantal personen”.³² De DSA erkent deze nuance, en stelt bijgevolg dat zogenaamde interpersoonlijke communicatiediensten – zoals e-mailproviders (bv. Outlook.com) en messaging-diensten (bv. Signal) – niet onder het toepassingsgebied vallen van onlineplatforms.³³

Deze nuance kwam verder onder de aandacht in 2024 na de arrestatie van Pavel Durov, CEO van messaging-app Telegram, door de Franse autoriteiten. Naar aanleiding van de arrestatie circuleerde het Franse parket een perscommuniqué waarin valt te lezen dat de aanhouding onder meer gelinkt is aan het ter beschikking stellen van een onlineplatform waarbinnen het mogelijk is om illegale transacties te verrichten in georganiseerde groepen.³⁴ Hoewel er binnen de DSA geen strafrechtelijk handavingsluit is voorzien, was wel een duidelijke DSA-retoriek merkbaar binnen de nieuwscyclus volgende op de arrestatie.³⁵ Gelet op het feit dat groepsgesprekken op Telegram tot 200.000 gebruikers kunnen tellen, rijst bijgevolg de vraag of de diensten van Telegram in aanmerking zouden kunnen komen als een onlineplatform in de zin van de DSA. De volgende twee vragen zijn daarbij van belang:

26 X, ‘Parler: Amazon to Remove Site from Web Hosting Service’ (BBC, 10 januari 2021) <<https://www.bbc.com/news/technology-55608081>> geraadpleegd op 5 december 2024.

27 Artikel 3(i), DSA.

28 Dit volgt tevens uit rechtsoverweging 13 *in fine*, DSA.

29 Rechtsoverweging 13, DSA; in dit geval zou de krant bijgevolg kwalificeren als een dienst van de informatiemaatschappij die geen tussenhandel-dienst uitmaakt.

30 In die zin, zie ook Caroline Cauffman en Catalina Goanta, ‘A New Order: The Digital Services Act and Consumer Protection’ (2021) 12 *European Journal of Risk Regulation* 758, 769.

31 Rechtsoverweging 14, DSA *juncto* artikel 3(k), DSA.

32 Rechtsoverweging 14, DSA.

33 Beide categorieën van dienstverleners komen veeleer in aanmerking als *mere conduit*-diensten.

34 Tribunal judiciaire de Paris, ‘Communiqué de Presse – TELEGRAM’ (2024) 1-2: ‘Complicité – Administration d’une plateforme en ligne pour permettre une transaction illicite en bande organisée’.

35 Zie bijvoorbeeld de reactie van Telegram naar aanleiding van de arrestatie: X, ‘Telegram News’ (Telegram, 25 augustus 2024) <<https://t.me/telegram/329>> geraadpleegd op 5 maart 2025: “Telegram abides by EU laws, including the Digital Services Act – its moderation is within industry standards and constantly improving”.

- (i) Is een kwalificatie als onlineplatform mogelijk wanneer informatie strikt genomen niet tot een onbeperkt aantal gebruikers wordt verspreid, maar weliswaar kan circuleren binnen een community die tot 200.000 gebruikers telt?
- (ii) Is er onder de DSA aanleiding voor een verschillende behandeling indien bij één community van 200.000 gebruikers de toegang tot geplaatste informatie wordt beheerd door een moderator, terwijl in een andere community van eveneens 200.000 gebruikers de geplaatste informatie publiek toegankelijk is?

Een grondige lezing van de DSA gebiedt dat er een analyse van de concreet aangeboden dienst moet volgen om tot een correcte kwalificatie te kunnen overgaan.³⁶ De vaststelling hierbij is dat Telegram een hybridemedium uitmaakt bestaande uit verschillende aparte diensten: interpersoonlijke communicatie, kleine groepsgesprekken, grote groepsgesprekken, en openbare kanalen.³⁷

- Voor een-op-een gesprekken, alsook voor kleine groepsgesprekken (*groups*), is de vaststelling dat deze dienst niet onder het toepassingsgebied van de DSA zal vallen maar dat het gaat over interpersoonlijke communicatie in de zin van rechtsoverweging 14 DSA.
- Voor zogenaamde “supergroepen” (*super groups*), die afgeschermd zijn en tot 200.000 leden kunnen bevatten, kan worden geargumenteed dat er niet langer sprake is van interpersoonlijke communicatie. Echter, strikt genomen is er bij dergelijke community's geen verspreiding onder een “*potentieel onbeperkt aantal personen*”, waardoor dit niet valt onder het begrip “onlineplatform” in de zin van artikel 3(i) DSA – een interpretatie die wordt bijgetreden door een woordvoerder van de Europese Commissie.³⁸
- Voor “kanalen” (*channels*), die openbaar zijn en een onbeperkt aantal gebruikers kunnen hebben, is er duidelijk wél functionaliteit die moet worden beschouwd als een onlineplatform in de zin van de DSA.

2.2.3.2 Onlinezoekmachines

De analyse van hosting-diensten die kwalificeren als *onlinezoekmachines* is meer rechtlijnig. Binnen de DSA komen dienstverleners in aanmerking als een onlinezoekmachine indien ze een dienst verrichten waarmee gebruikers informatie kunnen opzoeken door middel van zoekopdrachten op, in beginsel, alle websites.³⁹ Een karakteristieke eigenschap van zoekmachines is bijgevolg het indexeren van webinhoud, die vervolgens wordt gepresenteerd aan een

gebruiker aan de hand van een opgegeven trefwoord. Relevante voorbeelden zijn grote zoekmachines zoals Google Search en Bing, maar ook kleinere spelers op de markt zoals DuckDuckGo en Brave Search krijgen het label van onlinezoekmachine toegeschreven.

In de marge speelt er zich weliswaar een discussie af over de vraag of onlinezoekmachines overeenstemmen met hosting-diensten, dan wel caching-diensten. Wanneer we onlinezoekmachines meer technisch bekijken, dan lijkt ‘hosting’ inderdaad het best te passen omdat er in hoofdorde sprake is van de opslag van webcrawlgegevens. Sommige afzonderlijke functies kunnen echter ook in aanmerking komen als ‘caching’ (denk bijvoorbeeld aan Google Cache, zoals hoger besproken). Uiteindelijk zal de juiste kwalificatie afhangen van de concrete dienst die wordt geïmplementeerd, zoals de DSA ook zelf voorschrijft in rechtsoverweging 29. In navolging van *Google France en Google*⁴⁰ is het alleszins duidelijk dat een onlinezoekmachine zich kan beroepen op de voorwaardelijke aansprakelijkheidsvrijstelling voor hosting-diensten uit artikel 6 van de DSA en, bijgevolg, dat een onlinezoekmachine gezien kan worden als een deelcategorie van hosting-diensten.

2.2.4 Zeer grote onlineplatforms en zeer grote onlinezoekmachines

Binnen de DSA gaat er tot slot ook nog bijzondere aandacht uit naar *zeer grote onlineplatforms* en *zeer grote onlinezoekmachines*.⁴¹ In beide gevallen gaat het over respectievelijk een onlineplatform of een onlinezoekmachine die binnen de Europese Unie – en dus niet op globaal niveau⁴² – minstens 45 miljoen maandelijkse actieve gebruikers telt.⁴³ Het bekomen van een dergelijke kwalificatie verloopt niet automatisch, maar dient plaats te vinden aan de hand van een zogenaamd aanwijzingsbesluit van de Europese Commissie.⁴⁴ Wel is het zo dat onlineplatforms en onlinezoekmachines krachtens de transparantieplichtingen van artikel 24 DSA verplicht zijn om een

³⁶ Rechtsoverweging 29 in fine, DSA.

³⁷ Voor een uitgebreide analyse van Telegram onder de DSA, zie Tahireh Panahi et al., ‘Desinformationserkennung anhand von Netzwerkanalysen – ein Instrument zur Durchsetzung der Pflichten des DSA am Beispiel von Telegram’ in Michael Friedewald en Alexander Roßnagel (eds.), *Daten-Fairness in einer globalisierten Welt* (Nomos Verlag 2023) 344-348.

³⁸ X, ‘As France Cracks down on Telegram, EU Sits on the Sidelines’ (*Politico*, 29 augustus 2024) <<https://www.politico.eu/article/telegram-crackdown-eu-pavel-durov-paris-online-dsa/>> geraadpleegd op 5 december 2024.

³⁹ Artikel 3(j), DSA.

⁴⁰ Gevoegde zaken C-236/08 tot C-238/08, *Google France en Google* [2010] ECLI:EU:C:2010:159, paras 106-120.

⁴¹ Rechtsoverweging 76, DSA; artikel 33, DSA.

⁴² Zo telt het platform Reddit in totaal 430 miljoen globale gebruikers, maar ‘slechts’ 15,9 miljoen actieve EU-gebruikers. Daardoor kwalificeert Reddit als een onlineplatform onder de DSA, maar krijgt het niet het label “zeer groot” toegeschreven. De concrete informatie over het aantal gebruikers is publiek beschikbaar via de zesmaandelijkse rapporten die Reddit verplicht is om op te stellen krachtens de transparantieplichtingen van artikel 24 DSA: X, ‘Digital Services Act (DSA): Information for EU Users’ (*Reddit*, 13 januari 2025) <<https://support.reddithelp.com/hc/en-us/articles/23595536875796-Digital-Services-Act-DSA-Information-for-EU-users>> geraadpleegd op 13 februari 2025.

⁴³ In januari 2023 deelde de Europese Commissie een reeks richtsnoeren om te verduidelijken hoe ondernemingen het aantal actieve gebruikers van hun dienst moeten berekenen. Zo is een gebruiker enkel te beschouwen als een ‘actieve afnemer’ van de dienst indien die persoon in de voorafgaande periode van zes maanden minstens één keer met de dienst in aanraking kwam door bv. inhoud te bekijken of inhoud te delen. Dit impliceert m.a.w. dat een actieve afnemer van een dienst niet hetzelfde is als een geregistreerde gebruiker van die dienst: Europese Commissie, ‘Vragen en antwoorden over de identificatie en telling van actieve afnemers van de dienst in het kader van de digitale dienstenverordening’ (2023) <<https://ec.europa.eu/newsroom/dae/redirection/document/93781>> geraadpleegd op 13 februari 2025.

⁴⁴ Artikel 33(4), DSA.

zesmaandelijks rapport op te stellen om (onder andere) het gemiddelde aantal actieve gebruikers van de dienst in de EU in kaart te brengen.⁴⁵ Aan de hand van die informatie en in samenwerking met de relevante nationale digitaliedienstencoördinator, wordt de Europese Commissie op de hoogte gebracht van ondernemingen die de drempel van 45 miljoen actieve EU-gebruikers overschrijden.⁴⁶ Enkele recente ontwikkelingen werpen een nieuw licht op moeilijkheden gekoppeld aan de berekeningswijze van het gemiddelde aantal actieve gebruikers. Opeenvolgende transparantierapporten van Pornhub, XNXX, StripChat, en XVideos hebben allemaal opmerkelijke dalingen gerapporteerd wat betreft hun EU-gebruikers.⁴⁷ Zo rapporteerde XVideos op 17 februari 2025 dat ze maandelijks 31 miljoen EU-gebruikers hadden, tegenover 84 miljoen gerapporteerde gebruikers in augustus 2024.⁴⁸ Ook andere pornografische platformen meldde aanzienlijke dalingen, waarbij de drastische veranderingen in het aantal actieve EU-gebruikers werden toegeschreven aan een herziene methodologie voor het tellen van gebruikers die surfen in ‘incognito’-modus.⁴⁹ Voorheen werd van incognito-surfers aangenomen dat het ging om unieke gebruikers in de EU, terwijl de bijgewerkte berekeningsmethoden incognito-sessies in bepaalde mate buiten beschouwing laten. De vraag daarbij blijft natuurlijk of de meer conservatieve telmethoden effectief in overeenstemming zijn met de DSA en verhinderen dat gebruikers ‘dubbel geteld’ worden, of dat het eerder om een strategische keuze gaat om onder de drempel van 45 miljoen actieve EU-gebruikers te duiken, en finaal het label van ‘zeer groot’ te ontlopen. Het zal aan de EC zijn om meer details op te vragen over de gewijzigde methodologie en, indien nodig, de platformen ofwel terecht te wijzen, ofwel de kwalificatie te herbekijken. Niettegenstaande deze bemerkingen omtrent de berekeningswijze van het aantal actieve EU-gebruikers, dragen op het moment van schrijven 23 onlineplatforms en 2 on-

linezoekmachines het prefix “zeer groot” (zie tabel 1 op p. 92).⁵⁰

Hoewel de aanwijzingsbesluiten als dusdanig geen opvallende nieuwe inzichten bieden, valt wel op te merken dat de EC een duidelijk stramien hanteert waarbij er ook ruimte is voor een korte analyse van de aangeboden diensten. Op basis daarvan kan de EC bijvoorbeeld aangeven dat sommige diensten of subdiensten niet onder het aanwijzingsbesluit vallen. Zo wordt het socialemediaplatform Facebook bestempeld als een ‘zeer groot onlineplatform’, maar valt het uitwisselen van privéberichten via Facebook Messenger expliciet niet hieronder.⁵¹

Het is voorts nuttig om aan te stippen dat tegen de aanwijzingsbesluiten van de EC een beroep kan worden ingeleid voor het Gerecht. Verschillende ondernemingen – waaronder Amazon,⁵² Pornhub,⁵³ XNXX,⁵⁴ XVideos,⁵⁵ en Zalando⁵⁶ – hebben van die optie gebruikgemaakt. De ingediende verzoekschriften tonen aan dat de ondernemingen enerzijds de nietigverklaring van het aanwijzingsbesluit aanvragen, maar anderzijds in ondergeschikte orde soms ook verzoeken om specifieke verplichtingen van de DSA (tijdelijk) te schorsen.⁵⁷ Tot op heden slaagde geen enkel verzoek tot nietigverklaring van een aanwijzingsbesluit.

2.3 De DSA inhoudelijk bekeken

Op het moment van schrijven is er reeds veel inkt gevloeid over de inhoudelijke verplichtingen die voortvloeien uit de DSA.⁵⁸ Bijgevolg beperkt deze bijdrage zich enerzijds tot het aanreiken van een visueel overzicht van de meest

45 Artikel 24(2), DSA.

46 Artikel 24(4), DSA.

47 Anupriya Datta, ‘Porn Platforms Report EU User Collapse, May Dodge DSA Scrutiny’ (*Euractiv*, 18 februari 2025) <<https://www.euractiv.com/section/tech/news/porn-platforms-report-a-major-drop-in-eu-users-to-evade-dsa-responsibility/>> geraadpleegd op 21 februari 2025.

48 X, ‘Mandatory Information/Reports’ (*XVideos*, 17 februari 2025) <<https://info.xvideos.net/legal/mandatory-information>> geraadpleegd op 21 februari 2025.

49 Zie bijvoorbeeld X, ‘Mandatory Information/Reports’ (*XNXX*, 17 februari 2025) <<https://info.xnxx.com/legal/mandatory-information>> geraadpleegd op 21 februari 2025: “[...] we inform you that as of February 17, 2025, XNXX has 46 million average monthly recipients of the service in the European Union, calculated as an average over the period of the past six months. This number is significantly lower than our previously published numbers because it was impossible until recently to calculate an accurate number, due to the large proportion of people visiting with “incognito” browsers. We could only speculate as incognito users are normally undetectable, and repeated visits from them would be counted as extra visitors, meaning we would have had to guess a number ranging from roughly one to triple. [...] However we very recently found a way to account for them. We now know that in the EU, close to 35% of our users visit in incognito sessions (showing that visitors of adult site users are very concerned about their privacy...). This allowed us to calculate the more realistic number presented above.”

50 X, ‘Supervision of the Designated Very Large Online Platforms and Search Engines under DSA’ (Europese Commissie, 6 februari 2025) <<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>> geraadpleegd op 13 februari 2025.

51 Rechtsoverweging 7, Commission Decision of 25.4.2023 designating Facebook as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2756 final.

52 Zaak T-367/23, *Amazon EU/Commissie* [2023] ECLI:EU:T:2023:589; tegen de Beschikking van het Gerecht werd een hoger beroep ingeleid voor het Hof van Justitie: Zaak C-639/23 P(R), *Commissie/Amazon Services Europe* [2024] ECLI:EU:C:2024:277.

53 Zaak T-138/24, *Aylo Freesites/Commissie* [2024] ECLI:EU:T:2024:431; tegen de Beschikking van het Gerecht werd een hoger beroep ingeleid voor het Hof van Justitie: Zaak C-511/24 P(R), *Aylo Freesites/Commissie* [2024] ECLI:EU:C:2024:719.

54 Zaak T-486/24, *NKL Associates/Commissie* [2025] PB C, C/2024/6660.

55 Zaak T-139/24 R, *WebGroup Czech Republic/Commissie* [2024] ECLI:EU:T:2024:475.

56 Zaak T-348/23, *Zalando/Commissie* [2024] PB C, C/2023/314; tegen de Beschikking van het Gerecht werd een hoger beroep ingeleid voor het Hof van Justitie: Zaak C-647/23 P(I), *ELSi/Zalando en Commissie* [2024] ECLI:EU:C:2024:37.

57 Zo verzocht Amazon het Gerecht om de verplichting om een publiek toegankelijk advertentieregister bij te houden (artikel 39 DSA) op te schorten: Zaak T-367/23, *Amazon EU/Commissie* [2023] ECLI:EU:T:2023:589, paras 56 et seq.

58 Zie bijvoorbeeld de volgende artikelsgewijze commentaren: Folkert Wilman, Saulius Lukas Kalėda en Paul-John Loewenthal, *The EU Digital Services Act* (Oxford University Press 2024) 624 p.; Milos Novovic, *The EU Digital Services Act (DSA): A Commentary* (Kluwer Law International 2024) 560 p.; Ralf Müller-Terpitz en Markus Köhler, *Digital Services Act: Gesetz Über Digitale Dienste* (C.H. Beck 2023) 887 p.

Tabel 1 – Lijst van onlineplatforms en onlinezoekmachines die zijn aangewezen als ‘zeer groot’ onder de DSA

<i>Zeer grote onlineplatforms</i>	<i>Zeer grote onlinezoekmachines</i>
1. Alibaba AliExpress ¹	1. Bing ²⁴
2. Amazon Store ²	2. Google Search ²⁵
3. Apple AppStore ³	
4. Booking.com ⁴	
5. Facebook ⁵	
6. Google Maps ⁶	
7. Google Play ⁷	
8. Google Shopping ⁸	
9. Instagram ⁹	
10. LinkedIn ¹⁰	
11. Pinterest ¹¹	
12. Pornhub ¹²	
13. Shein ¹³	
14. Snapchat ¹⁴	
15. Stripchat ¹⁵	
16. Temu ¹⁶	
17. TikTok ¹⁷	
18. Wikipedia ¹⁸	
19. X (Twitter) ¹⁹	
20. XNXX ²⁰	
21. XVideos ²¹	
22. YouTube ²²	
23. Zalando ²³	

- 1 Commission Decision of 25.4.2023 designating AliExpress as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2736 final.
- 2 Commission Decision of 25.4.2023 designating Amazon Store as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2746 final.
- 3 Commission Decision of 25.4.2023 designating App Store as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2726 final.
- 4 Commission Decision of 25.4.2023 designating Booking.com as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2748 final.
- 5 Commission Decision of 25.4.2023 designating Facebook as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2756 final.
- 6 Commission Decision of 25.4.2023 designating Google Maps as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2737 final.
- 7 Commission Decision of 25.4.2023 designating Google Play as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2738 final.
- 8 Commission Decision of 25.4.2023 designating Google Shopping as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2733 final.
- 9 Commission Decision of 25.4.2023 designating Instagram as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2734 final.
- 10 Commission Decision of 25.4.2023 designating LinkedIn as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2735 final.
- 11 Commission Decision of 25.4.2023 designating Pinterest as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2729 final.
- 12 Het aanwijzingsbesluit van Pornhub is tot op heden niet gepubliceerd.
- 13 Commission Decision of 26.4.2024 designating SHEIN as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2024) 2842 final/2.
- 14 Commission Decision of 25.4.2023 designating Snapchat as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2730 final.
- 15 Het aanwijzingsbesluit van Stripchat is tot op heden niet gepubliceerd.
- 16 Het aanwijzingsbesluit van Temu is tot op heden niet gepubliceerd.
- 17 Commission Decision of 25.4.2023 designating TikTok as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2720 final.
- 18 Commission Decision of 25.4.2023 designating Wikipedia as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2742 final.
- 19 Commission Decision of 25.4.2023 designating Twitter as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2721 final.
- 20 Het aanwijzingsbesluit van XNXX is tot op heden niet gepubliceerd.
- 21 Het aanwijzingsbesluit van XVideos is tot op heden niet gepubliceerd.
- 22 Commission Decision of 25.4.2023 designating YouTube as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2725 final.
- 23 Commission Decision of 25.4.2023 designating Zalando as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2727 final.
- 24 Commission Decision of 25.4.2023 designating Bing as a very large online search engine in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2728 final.
- 25 Commission Decision of 25.4.2023 designating Google Search as a very large online search engine in accordance with Article 33(4) of Regulation (EU) 2022/2065 [2023] C(2023) 2731 final.

pertinente verplichtingen (zie *Figuur 1*), en anderzijds tot het aanbieden van een summier overzicht van de drie belangrijkste facetten van de DSA:

- (i) Het *safe harbour*-regime, op grond waarvan tussenhandeldiensten een voorwaardelijke vrijstelling van aansprakelijkheid kunnen bekomen wanneer gebruikers illegale inhoud via de dienst verspreiden.
- (ii) De *zorgvuldigheidsverplichtingen* die rusten op tussenhandeldiensten en die beogen bij te dragen tot een meer transparante en veilige onlineomgeving.
- (iii) De *risicobeoordelings-* en *risicobeperkingsverplichtingen* voor zeer grote onlineplatforms en zeer grote onlinezoekmachines, op basis waarvan dergelijke dienstverleners systemische risico's (bv. de aantasting van fundamentele rechten) in kaart moeten brengen en inperken (zie *Figuur 1* op p. 94).

2.3.1 Het voorwaardelijk aansprakelijkheidsvrijstellingsregime

De DSA bevat een voorwaardelijke aansprakelijkheidsvrijstelling – het zogenaamde *safe harbour*-regime – voor de drie verschillende categorieën van tussenhandeldiensten.⁵⁹ Op basis daarvan kunnen de dienstverleners ontsnappen aan hun aansprakelijkheid voor de illegale inhoud die gebruikers via de dienst verspreiden.⁶⁰ Hoewel de voorwaarden niet volledig gelijklopen, kan voor *mere conduit*- en *caching*-dienstverleners worden opgemerkt dat de toepassing van de vrijstellingsregeling in hoofde afhangt van een vereiste van neutraliteit bij het doorgeven en (tijdelijk) opslaan van informatie van gebruikers: deze twee soorten dienstverleners kunnen aansprakelijkheidsclaims voor illegale inhoud ontlopen indien ze de inhoud van hun gebruikers louter passief doorgeven of hosten.⁶¹ Omgekeerd, daarentegen, wanneer de dienstverlener actief wijzigingen doorvoert aan de inhoud, kan de dienstverlener dit regime niet genieten. Voor *hosting*-diensten is de regeling wat uitgebreider en geldt er een bijkomende vereiste van gebrek aan kennis hebben van de illegale inhoud: er kan enkel een vrijstelling worden verkregen zolang de dienstverlener geen kennis heeft van illegale inhoud die op het platform ter beschikking wordt gesteld.⁶² Bij uitbreiding moeten, zodra de dienstverlener op de hoogte wordt gebracht van de illegale inhoud, de nodige stappen worden genomen om de illegale inhoud te verwijderen of ontoegankelijk te maken.⁶³ Een bijkomende (en tevens ook nieuwe) aanvulling op dit regime vloeit voort uit artikel 7 van de DSA, dat in de lite-

atuur bekendstaat als de *Good Samaritan*-bepaling.⁶⁴ Deze bepaling stelt dat tussenhandeldiensten die te goeder trouw en op vrijwillige basis bepaalde activiteiten stellen om illegale inhoud te detecteren en te verwijderen, op grond van dergelijke activiteiten niet de toegang tot de voorwaardelijke aansprakelijkheidsvrijstelling verliezen.⁶⁵ Dit houdt bijgevolg in dat dienstverleners zich bijvoorbeeld mogen verlaten op:

- De *automatische filtering* van content (bv. het Content ID-systeem waarmee YouTube tracht te identificeren of auteursrechtelijk beschermd materiaal wordt gebruikt in filmpjes).
- De *handmatige moderatie* van content (bv. het inzetten van moderatoren op een socialemidiaplatform om beelden van seksueel misbruik van minderjarigen of extremistische inhoud te verwijderen).
- Een *rapporteringssysteem* waarmee gebruikers binnen een platformgeving melding kunnen maken van andere accounts die illegale content verspreiden.

Tot slot verduidelijkt artikel 8 van de DSA ook dat er geen algemene verplichting rust op aanbieders van tussenhandeldiensten om door gebruikers doorgegeven informatie of opgeslagen informatie actief te checken op het al dan niet illegale karakter ervan.⁶⁶

Wat betreft de bestrijding van illegale inhoud, voorziet de DSA in twee aparte routes:

- (i) Voor alle tussenhandeldiensten geldt er een verplichting om illegale inhoud te verwijderen of ontoegankelijk te maken naar aanleiding van een bevel van een nationale gerechtelijke of administratieve autoriteit. Hierbij is het onder meer vereist dat het bevel in kwestie een duidelijke rechtsgrond en een motivering bevat, alsook de relevante informatie om de illegale inhoud terug te vinden (bv. een hyperlink).
- (ii) *Hosting-diensten* en *onlineplatforms* moeten tevens een zogenaamd *kennisgevings- en actiemechanisme* ter beschikking stellen aan hun gebruikers.⁶⁷ Aan de hand daarvan kunnen gebruikers zelf illegale inhoud melden aan de dienstverlener en, indien de melding voldoende nauwkeurig en gemotiveerd is, moet de dienstverlener hiertegen optreden door de inhoud ofwel te verwijde-

⁵⁹ Artikels 4-10, DSA.

⁶⁰ Peter Rott, 'New Liability of Online Marketplaces Under the Digital Services Act?' (2022) 30 *European Review of Private Law* 1039, 1045.

⁶¹ Artikels 4-5, DSA.

⁶² Artikel 6, DSA; Ceyhun Necati Pehlivan en Peter Church, 'The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability' (2023) 4 *Global Privacy Law Review* 53, 55.

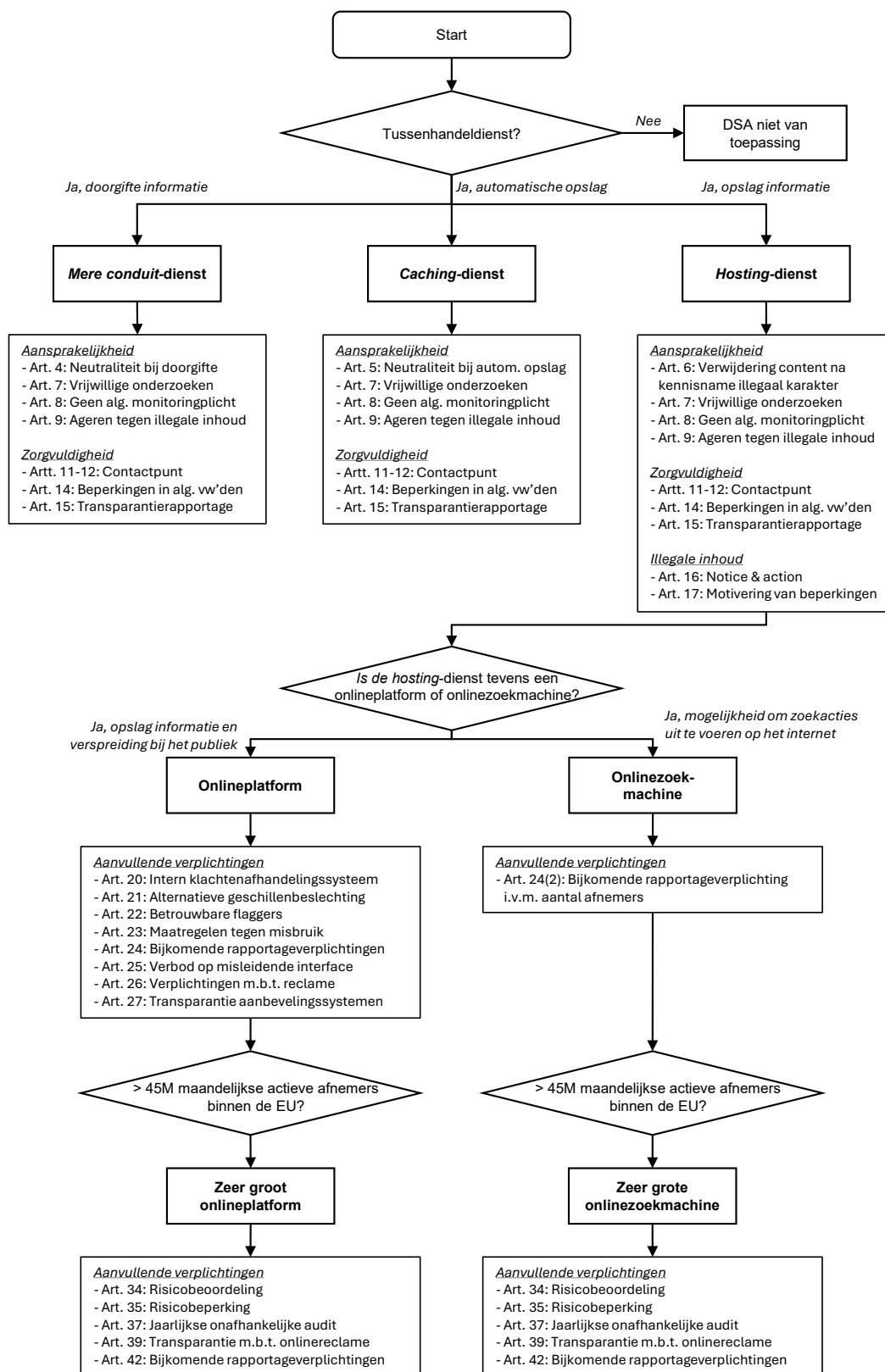
⁶³ Noor de Werd en Tosca Bokhove, 'Wat is de rol en verantwoordelijkheid van online platforms in de digitale strijd tegen namaakproducten?' [2022] 1 *Computerrecht* 17, 21-22.

⁶⁴ Folkert Wilman, 'De Digital Services Act (DSA): een belangrijke stap naar betere regulering van onlinedienstverlening' (2022) 28 *Nederlands tijdschrift voor Europees Recht* 220, 223.

⁶⁵ Caroline Cauffman en Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12 *European Journal of Risk Regulation* 758, 765 en 769.

⁶⁶ Zie tevens rechtsoverweging 30, DSA.

⁶⁷ Artikel 16, DSA; rechtsoverwegingen 50-53, DSA; voor een kritische analyse, zie Pieter Wolters en Raphaël Gellert, 'Het "notice and action-mechanisme" van de DSA: een adequaat evenwicht tussen de betrokken belangen?' (2022) 218 *Computerrecht* 391, 397-398; Pieter Wolters en Raphaël Gellert, 'Towards a Better Notice and Action Mechanism in the DSA' (2023) 14 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 403, 411-413.

Figuur 1 – Stroomdiagram van de voornaamste verplichtingen opgenomen in de DSA¹

¹ De figuur is een eigen ontwerp van de auteurs.

ren ofwel ontoegankelijk te maken.⁶⁸ Voor *onlineplatforms* geldt er voorts een bijkomende verplichting krachtens artikel 22 DSA om *betrouwbare flaggers*⁶⁹ in te schakelen, wiens specifieke taak het is om illegale inhoud op te sporen en te melden. De meldingen van deze betrouwbare flaggers moeten prioritair worden opgevolgd, aldus de bewoordingen van de DSA.⁷⁰

2.3.2 Zorgvuldigheidsverplichtingen

De DSA maakt in totaal tien keer melding van het begrip 'zorgvuldigheidsverplichtingen'. Over welke concrete verplichtingen het effectief gaat, en hoe ver de verplichtingen reiken, is niet altijd even duidelijk. Niettemin, en zonder in detail te treden, zijn er een drietal overkoepelende zorgvuldigheidsverplichtingen die gelden voor alle tussenhandeldiensten. Deze algemeen toepasselijke verplichtingen worden aangevuld met een reeks bijkomende zorgvuldigheidsverplichtingen die louter van toepassing zijn op (zeer grote) onlineplatforms en (zeer grote) onlinezoekmachines. Ten eerste gaat het over het aanduiden van een *centraal contactpunt* voor zowel autoriteiten als afnemers van de dienst.⁷¹ Dit maakt immers vlotte communicatie mogelijk, wat pertinent is om illegale inhoud zo snel mogelijk te bestrijden.⁷²

Ten tweede geldt er een verplichting om *beperkingen op het gebruik van de dienst* via de algemene voorwaarden te verduidelijken.⁷³ Hierbij dient er specifieke aandacht uit te gaan naar enerzijds inhoudsmoderatie en anderzijds de procedures om klachten intern af te handelen. Via de algemene voorwaarden beschikken dienstverleners over de mogelijkheid om aan te geven welke inhoud gebruikers mogen opslaan of verspreiden. Zo informeert het livestreamingplatform Twitch haar gebruikers via "Community Guidelines" dat het (onder meer) verboden is om zelfdestructief gedrag⁷⁴ te promoten, bedreigingen te uiten, aan te zetten tot geweld of extremisme, seksueel expliciete inhoud te streamen, auteursrechtelijk beschermde content van anderen af te spelen, of persoonlijk identifi-

ceerbare informatie te delen.⁷⁵ De dienstverstrekker kan op diezelfde wijze ook signaleren aan afnemers van de dienst welke concrete gevolgen eraan zijn gekoppeld wanneer de gestelde voorwaarden met de voet worden getreden. Gewoonlijk is er wat dit betreft een spectrum aan sancties voorhanden, naargelang de ernst van de inbreuk. Typerend gaat het over het geven van een waarschuwing, het opleggen van een tijdelijke accountschorsing, of – in situaties waarin er nultolerantie heerst – het toepassen van een onmiddellijke accountverbanning.⁷⁶

Ten derde moeten tussenhandeldiensten gevolg geven aan *transparantierapportageverplichtingen*.⁷⁷ Op basis daarvan zijn dienstverleners verplicht om minstens op jaarbasis een rapport op te stellen over de inhoudsmoderatie die ze hebben uitgevoerd. De DSA vergt dat het rapport duidelijkheid moet scheppen over (onder meer) het aantal ontvangen bevelen van nationale autoriteiten,⁷⁸ de verschillende types illegale inhoud waarmee de dienstverlener werd geconfronteerd, de interventies getroffen naar aanleiding van de illegale inhoud, het aantal ontvangen klachten, en het concrete gebruik van contentmoderatietools. Wat betreft de aanvullende zorgvuldigheidsverplichtingen, kwam in de vorige sectie reeds de verplichte implementatie van een kennisgevings- en actiemechanisme voor hosting-diensten ter sprake.⁷⁹ Voor onlineplatforms zijn er voorts nog bijkomende verplichtingen opgenomen in artikels 20-32 DSA met betrekking tot (onder andere) *dark patterns*, het gebruik van reclame, en transparantie omtrent aanbevelingssystemen. De aanvullende zorgvuldigheidsverplichtingen voor VLOP's en VLOSE's zijn dan weer terug te vinden in artikels 33-43 DSA.

2.3.3 Risicobeoordelingen en risicobeperkingen

Tot slot zijn er aanvullende verplichtingen voor aanbieders van VLOP's en VLOSE's om zogenaamde systeemrisico's te ondervangen. Wat concreet valt te verstaan onder een systeemrisico, wordt verduidelijkt in rechtsoverwegingen 80-83 van de DSA, waar er sprake is van een vierledige indeling:

- Risico's gelinkt aan de *verspreiding van illegale inhoud*.⁸⁰ Gelet op de grote gebruikersaantallen, is de impact qua verspreiding van illegale inhoud aanzienlijk gewichtiger bij VLOP's en VLOSE's omdat de inhoud snel en bovendien ook op veel grotere schaal kan worden gedeeld, bijvoorbeeld via gebruikers met vele 'volgers'.
- Risico's gekoppeld aan *fundamentele rechten van individuen*.⁸¹ Het risico bestaat dat de werking van algoritmes, aanbevelingssystemen, of contentmoderatietie-

68 Artikel 17, DSA; de website van de Europese Commissie voorziet in een 'DSA Transparency Database', waarin gebruikers de aangehaalde motivering voor de (automatische) moderatie van inhoud kunnen opzoeken: Europese Commissie, 'DSA Transparency Database' (Europese Commissie, 20 februari 2025) <<https://transparency.dsa.ec.europa.eu/statement>> geraadpleegd op 21 februari 2025.

69 Naomi Appelman en Paddy Leerssen, 'On "Trusted" Flaggers' (2022) 24 *Yale Journal of Law and Technology* 452, 455-457 geven een overzicht van het beleid van verschillende populaire onlineplatforms omtrent 'betrouwbare flaggers'.

70 Artikel 22, DSA.

71 Artikels 11-12, DSA.

72 Folkert Wilman, 'De Digital Services Act (DSA): een belangrijke stap naar betere regulering van onlinedienstverlening' (2022) 28 *Nederlands tijdschrift voor Europees Recht* 220, 225.

73 Artikel 14, DSA; Mathieu Fasel en Sophie Weerts, 'Can Facebook's Community Standards Keep up with Legal Certainty? Content Moderation Governance under the Pressure of the Digital Services Act' (2024) 16 *Policy & Internet* 588, 593-594.

74 Bijvoorbeeld het promoten van eetstoornissen of het aanzetten tot zelfverminking.

75 X, 'Communityrichtlijnen: Inleiding tot veiligheid op Twitch' (Twitch, 20 januari 2025) <https://safety.twitch.tv/s/article/Community-Guidelines?language=nl_NL> geraadpleegd op 19 februari 2025.

76 *Ibid.*

77 Artikel 15, DSA.

78 Artikel 15(1)(a), DSA.

79 Zie hoger bij Subsectie 2.3.1 *Het voorwaardelijk aansprakelijkheidsvrijstellingsregime*.

80 Rechtsoverweging 80, DSA.

81 Rechtsoverweging 81, DSA.

systemen binnen de platformomgeving een negatieve impact heeft op de grondrechten van EU-burgers, zoals de vrijheid van meningsuiting, het recht op gegevensbescherming, het recht op non-discriminatie, en de pluraliteit van media.⁸²

- Risico's die verband houden met de *verstoring van democratische processen en de openbare veiligheid*.⁸³ Deze categorie omvat situaties zoals de verstoring van verkiezingen – denk daarbij aan de verkiezingsinterferentie die aan het licht kwam via het Cambridge Analytica-schandaal⁸⁴ – en het manipuleren van maatschappelijk debatten. Dit kan bijvoorbeeld plaatsvinden op basis van desinformatie of zogenaamde *influence campaigns*.⁸⁵ Ook bedreigingen van de openbare veiligheid door het organiseren van gewelddadige acties via VLOP's en VLOSE's – zoals het aansporen tot de bestorming van het Amerikaanse Capitool op 6 januari 2021 via socialemediaberichten⁸⁶ – vallen hieronder.
- Risico's die samenhangen met *negatieve gevolgen voor de volksgezondheid en het welzijn van individuen*.⁸⁷ Binnen deze vierde categorie verschuilt het systeemrisico zich in de verspreiding van misleidende (gezondheids)-informatie, het bevorderen van verslavend gedrag via interfaces die manipulatieve elementen bevatten, als ook het aanzetten tot schadelijke trends. Een passend voorbeeld hiervan is de *Blue Whale Challenge* die medio 2016 via sociale media verspreidde, waarbij minderjarigen werden aangemoedigd om opdrachten uit te voeren die zelfverminking inhielden en aanzetten tot zelfdoding. Ook kan worden gedacht aan de *Tide Pod Challenge* die in 2018 via TikTok circuleerde en waarbij jongeren elkaar uitdaagden om vaatwastabletten ('*tide pods*' in het Engels) te consumeren. Een andere noemenswaardige trend die binnen deze categorie past is het fenomeen van *doxing* (soms ook gespeld als *doxxing*), waarbij een gebruiker van een platform de persoonsgegevens (bv. adresinformatie) van iemand deelt, met de intentie om andere gebruikers aan te zetten tot intimidatie, het versturen van haatdragende berichten, of andere vormen van cybergeweld.

In het licht van de hogervermelde risico's hebben VLOP's en VLOSE's bijgevolg een verplichting om minstens jaarlijks een beoordeling van mogelijke systeemrisico's uit te voeren van

hun dienst en de daaraan gekoppelde algoritmische systemen.⁸⁸ Binnen die risicobeoordeling moet er bijzondere aandacht uitgaan naar de werking van aanbevelingssysteem, reclamesystemen, contentmoderatiesystemen en, meer algemeen, de datagerelateerde praktijken van de dienstverlener. Uit de rapporten volgt dat de dienstverleners uiteenlopende methodologieën hanteren om systeemrisico's in kaart te brengen en dat ze teruggrijpen naar specifieke industrie-standaards⁸⁹ om risicoanalyses uit te voeren. Dit verklaart waarom verschillende rapporten uitgebreide waarschijnlijkheidsmatrices en ernstmatrices bevatten.⁹⁰

Aan de hand van bovenstaande risicobeoordeling, geldt er ook een bijkomende verplichting om de geïdentificeerde risico's op een redelijke, evenredige, en doeltreffende wijze te ondervangen.⁹¹ Deze verplichting tot het voorzien in risicobeperkingsmaatregelen geeft aan dat maatregelen bijvoorbeeld kunnen bestaan uit het aanpassen van de werking van de dienst, het bijstellen van de algemene voorwaarden, en het aanpassen van de onderliggende algoritmische systemen. Het valt daarbij vooral op dat zowel de identificatie van systeemrisico's als de beperking van die risico's in de eerste plaats bij de VLOP's en VLOSE's zelf ligt, wat logisch is aangezien zij als enige volledig toegang hebben tot de relevante onderliggende gegevens om de risico's in kaart te brengen.⁹² Wel is het zo dat VLOP's en VLOSE's ook minstens één keer per jaar een onafhankelijke audit moeten ondergaan, al is het weliswaar moeilijk om hier toezicht op uit te oefenen (bv. vanwege moeilijkheden om toegang te krijgen tot de informatie die nodig is om de audits te beoordelen, of omdat er specifieke kennis nodig is van de gehanteerde auditmethoden).⁹³

Op het moment van schrijven heeft de Europese Commissie 10 formele procedures ingeleid tegen VLOP's en VLOSE's (zie *Tabel 2*):⁹⁴

82 Zie bijvoorbeeld het overzicht opgenomen in AliExpress, 'Digital Services Act: Risk Assessment and Mitigation Measures Report 2024' (2024) Risk assessment report 1, 50-53.

83 Rechtsoverweging 82, DSA.

84 Christoph Busch en Vanessa Mak, 'Putting the Digital Services Act in Context: Bridging the Gap Between EU Consumer Law and Platform Regulation' (2021) 10 *Journal of European Consumer and Market Law* 109, 109.

85 Niels Nagelhus Schia en Lars Gjesvik, 'Hacking Democracy: Managing Influence Campaigns and Disinformation in the Digital Age' (2020) 5 *Journal of Cyber Policy* 413, 414.

86 Craig Timberg, Elizabeth Dwoskin en Reed Albergotti, 'Inside Facebook, Jan. 6 violence fueled anger, regret over missed warning signs' (*Washington Post*, 20 oktober 2021) <<https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook/>> geraadpleegd op 18 februari 2025.

87 Rechtsoverweging 83, DSA.

88 Voor een overzicht van ingediende rapporten, zie Europese Commissie, 'How the Digital Services Act enhances transparency online' (*Europese Commissie*, 12 februari 2025) <<https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency#ecl-inpage-lsets&q=>> geraadpleegd op 19 februari 2025.

89 Zoals ISO-standaard 31000:2018 - Risk management: Facebook, 'Systemic Risk Assessment and Mitigation Report for Facebook' (2024) Risk assessment report 1, 13.

90 Zie bijvoorbeeld X, 'Report Setting Out the Results of Twitter International Unlimited Company Risk Assessment Pursuant to Article 34 EU Digital Services Act' (2023) Risk assessment report 1, 14-19.

91 Artikel 35, DSA.

92 Caroline Cauffman en Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12 *European Journal of Risk Regulation* 758, 770-771.

93 Artikel 37, DSA; om het proces van onafhankelijke controles te stroomlijnen, heeft de EC in 2023 ook een gedelegeerde verordening aangenomen om meer duidelijkheid te scheppen omtrent de uit te voeren controles en controlemethodes. Ook voorziet de gedelegeerde verordening in een model van een controlerapport en controle-uitvoeringsrapport: Gedelegeerde Verordening (EU) 2024/436 van de Commissie van 20 oktober 2023 tot aanvulling van Verordening (EU) 2022/2065 van het Europees Parlement en de Raad wat betreft voorschriften voor de uitvoering van controles van aanbieders van zeer grote onlineplatforms en van zeer grote onlinezoekmachines [2024] *PB L* 2024/436.

94 Voor een overzicht van de lopende procedures, zie X, 'European Commission - Enforcement with Regard to Very Large Online Platforms and Search Engines' (*DSC Database*, 6 februari 2025) <<https://dscdb.edri.org/EuropeanCommission>> geraadpleegd op 21 februari 2025.

Tabel 2 – Overzicht van procedures ingeleid door de EC op basis van de DSA

Datum	Dienstverlener	Aanknopingspunten
18-dec-2023	X ¹	- Risicobeperking - Inhoudsmoderatie - <i>Dark patterns</i> - Transparantie m.b.t. reclame - Toegang tot gegevens voor onderzoekers
19-feb-2024	TikTok ²	- Verspreiding van illegale inhoud en desinformatie - Bescherming van minderjarigen - Toegang tot gegevens voor onderzoekers
14-mrt-2024	AliExpress ³	- Risicobeperking m.b.t. consumentenbescherming - Toegang tot gegevens voor onderzoekers
22-apr-2024	TikTok ⁴	- Negatieve effecten op mentaal welzijn - Stimulering van verslavend gedrag
30-apr-2024	Facebook ⁵	- Risicobeperking m.b.t. de integriteit van verkiezingen - Verspreiding van illegale inhoud en desinformatie - Toegang tot gegevens voor onderzoekers
30-apr-2024	Instagram ⁶	- Risicobeperking m.b.t. de integriteit van verkiezingen - Verspreiding van illegale inhoud en desinformatie - Bescherming van minderjarigen - Toegang tot gegevens voor onderzoekers
16-mei-2024	Facebook ⁷	- Bescherming van minderjarigen - Keuze-optie advertenties zonder profilering
16-mei-2024	Instagram ⁸	- Bescherming van minderjarigen - Keuze-optie advertenties zonder profilering
31-okt-2024	Temu ⁹	- Risicobeperking m.b.t. consumentenbescherming - <i>Dark patterns</i> - Werking van aanbevelingssystemen - Toegang tot gegevens voor onderzoekers
17-dec-2024	TikTok ¹⁰	- Werking van aanbevelingssystemen - Beleid inzake politieke reclame en betaalde politieke inhoud

1 Europese Commissie, 'Commission opens formal proceedings against X under the Digital Services Act' (*Europese Commissie*, 18 december 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> geraadpleegd op 19 februari 2025.

2 Europese Commissie, 'Commission opens formal proceedings against TikTok under the Digital Services Act' (*Europese Commissie*, 19 februari 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926> geraadpleegd op 19 februari 2025.

3 Europese Commissie, 'Commission opens formal proceedings against AliExpress under the Digital Services Act' (*Europese Commissie*, 14 mei 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1485> geraadpleegd op 19 februari 2025.

4 Europese Commissie, 'Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU' (*Europese Commissie*, 22 april 2024) <https://ec.europa.eu/commission/presscorner/detail/en/p_24_2227> geraadpleegd op 19 februari 2025.

5 Europese Commissie, 'Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act' (*Europese Commissie*, 30 april 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373> geraadpleegd op 19 februari 2025.

6 *Ibid.*

7 Europese Commissie, 'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram' (*Europese Commissie*, 16 mei 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664> geraadpleegd op 19 februari 2025.

8 *Ibid.*

9 Europese Commissie, 'Commission opens formal proceedings against Temu under the Digital Services Act' (*Europese Commissie*, 31 oktober 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5622> geraadpleegd op 21 februari 2025.

10 Europese Commissie, 'Commission opens formal proceedings against TikTok on election risks under the Digital Services Act' (*Europese Commissie*, 17 december 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487> geraadpleegd op 19 februari 2025.

3 Tussen contentmoderatie en algospeak

3.1 Niveaus van contentmoderatie

Bij wijze van *capita selecta* gaat er in deze sectie bijzondere aandacht uit naar contentmoderatie. Onlineplatforms en onlinezoekmachines voorzien gewoonlijk in een meerlagige vorm van contentmoderatie, en om dit te illustreren refereren we aan een fictief socialemediaplatform. Hierbij kunnen we een viertal niveaus van moderatie onderscheiden,⁹⁵ waarbij de opstapeling van deze vier lagen zorgt voor de nodige flexibiliteit om ook rekening te houden met individuele gebruikersvoorkeuren of de cultuur die heerst binnen een specifieke community.

De eerste verdedigingslinie bestaat erin om heldere *algemene voorwaarden* op te stellen,⁹⁶ die duidelijk signaleren welke inhoud is toegestaan binnen de platformomgeving en welke gedragingen verboden zijn. Op die manier geven de algemene voorwaarden vorm aan de inhoudelijke onderbouw van de platformomgeving en scheppen ze een duidelijk verwachtingspatroon voor gebruikers. De algemene voorwaarden hebben bijgevolg vooral een preventieve werking, in die zin dat er geen illegale inhoud op het platform zou mogen verschijnen in de eerste plaats. Tegelijk sturen de algemene voorwaarden de drie andere niveaus van contentmoderatie aan en communiceren ze op een heldere manier dat als er regels worden overtreden, daar ook tegen zal worden opgetreden.

De tweede laag van moderatie heeft betrekking op *platformbrede tools en processen*. In hoofddeorde zal het hierbij gaan over de geautomatiseerde detectie van illegale inhoud via AI-systemen.⁹⁷ Dergelijke tools kunnen problematische inhoud (bv. haatdragende of extremistische inhoud) aanduiden voor een menselijke check-up of een volledig geautomatiseerde beslissing nemen over het verwijderen van inhoud.⁹⁸ Voorts kunnen hier opnieuw de kennisgevings- en actiemechanismen worden vermeld, aan de hand waarvan gebruikers zelf binnen de platformomgeving inhoud kunnen signaleren die mogelijk tegen de algemene voorwaarden indruist.⁹⁹ Tot slot is er binnen deze tweede laag ook ruimte voor menselijke moderatie,

in de vorm van *factcheckers* of *content flaggers*,¹⁰⁰ wiens taak het is om de door gebruikers geposte inhoud te controleren, de meldingen van gebruikers via het kennisgevings- en actiemechanisme op te volgen, of de door AI-systemen als problematisch gelabelde inhoud te dubbelchecken. Op basis van deze processen kunnen aansluitend ook concrete follow-upacties worden gekoppeld, zoals het uitreiken van een waarschuwing of het opleggen van een (tijdelijke) accountverbanning. Echter zijn deze automatische moderatie- en meldingssystemen niet altijd waterdicht. De afhandeling van meldingen kan vertraging oplopen, zonder verdere uitleg worden afgewezen, of in de vergetelheid raken. Een voorbeeld hiervan vinden we in X (voorheen Twitter), waar Elon Musk na de overname de moderatie sterk inperkte en meldingen over haatdragende inhoud en desinformatie vaak onbehandeld bleven.¹⁰¹

Als derde laag vinden we daarom *moderatietools op het niveau van individuele kanaalpagina's of profielpagina's* terug. Op dit niveau heeft de eigenaar van het kanaal of de profielpagina bijkomende ruimte om contentmoderatie uit te voeren binnen zijn of haar specifieke community,¹⁰² boven op de platformbrede moderatiemechanismen. Een typische maatregel op dit niveau is dat kanaaleigenaars bepaalde andere gebruikers kunnen machtigen om als moderator op te treden en om zo de platformbrede regels evenals kanaalspecifieke regels – zoals strengere chatregels – af te dwingen. Dergelijke moderators beschikken gewoonlijk over een aparte interface waarmee ze de inhoud geplaatst door gebruikers op het kanaal of de profielpagina kunnen monitoren en, waar nodig, gebruikers een time-out kunnen geven of verbannen van het kanaal. In het verlengde hiervan bestaan er ook geautomatiseerde moderatietools (*auto mods*), die bepaalde trefwoorden of spamberichten in real-time kunnen detecteren en verbergen op de kanaalpagina's. De mate van gestrengheid waarmee er gemodereerd wordt, hangt natuurlijk af van de specifieke kanaaleigenaars en vooral ook de inhoud van het kanaal. Daarbij gelden de platformbrede regels als een absolute ondergrens. Het grote voordeel van de gecombineerde aanpak van enerzijds moderatie op het niveau van individuele kanalen en anderzijds platformbrede moderatie, is dat het toestaat om beter rekening te houden met de inhoud van elk specifiek kanaal. Zo zal een YouTube-kanaal dat zich richt op minderjarige gebruikers nood hebben aan strengere individuele moderatie in vergelijking met een videokanaal gericht op een volwassen doelpubliek.

⁹⁵ Zie bijvoorbeeld Twitch, 'Transparency Reports' (Twitch, 24 januari 2025) <https://safety.twitch.tv/s/article/Transparency-Reports?language=en_US> geraadpleegd op 20 februari 2025.

⁹⁶ Cf. artikel 14, DSA.

⁹⁷ Tarleton Gillespie, 'Content Moderation, AI, and the Question of Scale' (2020) 7 *Big Data & Society* 1, 2; voor een overzicht van de voornaamste algoritmische contentmoderatietechnieken, zie Robert Gorwa, Reuben Binns en Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 *Big Data & Society* 1, 3-5.

⁹⁸ Ter illustratie: in de periode van 1 april 2024 tot 30 september 2024 verwijderde Instagram 12.136.947 contentitems, waarvan 10.535.490 (86,81%) via geautomatiseerde tools: Instagram, 'Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Instagram' (2024) Transparency report 1, 11-12.

⁹⁹ Ter illustratie: in de periode van 1 april 2024 tot 30 september 2024 onderzocht Instagram 1.543.038 meldingen van gebruikers over illegale inhoud. In 268.853 (17,42%) van deze gevallen werd de gemelde inhoud nadien terug online geplaatst na een evaluatie van de melding: *Ibid.*, 15.

¹⁰⁰ Cf. artikel 22, DSA.

¹⁰¹ Valerie Vanhelden, 'Europese Commissie roept Elon Musk op het matje voor desinformatie over Israëlisch-Palestijns conflict op X' (VRT Nieuws, 12 oktober 2023) <<https://www.vrt.be/vrtnws/nl/2023/10/12/europese-commissie-x-desinformatie-en-illegale-inhoud/>> geraadpleegd 5 maart 2025.

¹⁰² Denk daarbij bijvoorbeeld aan een YouTube-kanaal, een Instagram-pagina, of een online discussieforum.

Als vierde laag geven onlineplatforms gewoonlijk ook een zekere mate van *contentmoderatie in de handen van individuele gebruikers*. Wat dit betreft kunnen gebruikers binnen hun account bijvoorbeeld aangeven welke inhoud ze zelf niet wensen te zien. Typerende middelen waarover gebruikers beschikken, zijn het blokkeren (of tijdelijk dempen) van andere gebruikers, of het gebruiken van chatfilters waarmee ze bepaalde thema's uit hun nieuwsfeed kunnen houden. Ook de typische “viewer discretion is advised”-pop-ups kunnen we bij deze categorie onderbrengen. Dit lukt niet altijd op een goede manier. Recentelijk ervoer Instagram een storing waardoor gebruikers, ondanks geactiveerde gevoelige-inhoudfilters, wereldwijd werden overspoeld met gewelddadige en grafische video's in hun Reels-feed. Hoewel gebruikers dus de tools hebben om ongewenste inhoud te filteren, kunnen technische storingen deze maatregelen ondermijnen, wat leidt tot ongewenste blootstelling aan schadelijke content.¹⁰³

3.2 Moderatie van illegale versus schadelijke inhoud

Hoewel onlineplatforms en onlinezoekmachines duidelijk gerechtigd zijn om contentmoderatietools aan te wenden om illegale inhoud te verwijderen, is de situatie aanzienlijk minder duidelijk wanneer het gaat over de behandeling van *schadelijke inhoud*, zoals desinformatie, misinformatie, en nepnieuws.¹⁰⁴ De DSA stuit wat dit betreft immers op nieuwe problemen: de invulling van dergelijke begrippen laten de nodige ruimte voor interpretatie en zijn – in vergelijking met het begrip ‘illegale inhoud’¹⁰⁵ – daardoor aanzienlijk lastiger om af te bakenen. Zo kunnen er bij de interpretatie territoriale verschillen opduiken, aangezien het ontbreken van Europese definities van deze begrippen ertoe kan leiden dat wat in de ene lidstaat verboden is, niet per se in een andere lidstaat verboden hoeft te zijn. Het gevolg daarvan is dat onlineplatforms en onlinezoekmachines bij de opvolging van hun zorgverplichtingen op een dilemma stuiten wanneer er twijfel bestaat over het al dan niet schadelijke karakter van bepaalde inhoud: ofwel de inhoud verwijderen en daardoor mogelijk het recht op vrije meningsuiting van gebruikers inperken, ofwel de inhoud onaangeroerd laten en het risico lopen om door nationale regulerende of de Europese Commissie te worden beboet. In dergelijke situaties zal het niet verbazen dat dienstverleners er voor-

zichtigheidshalve eerder de voorkeur aan geven om de inhoud in kwestie te verwijderen of ontoegankelijk te maken, veeleer dan zich blootstellen aan de sancties van de DSA.¹⁰⁶

Een aantal initiatieven binnen de platformomgeving tracht aan die bezorgdheden tegemoet te komen en een beter evenwicht te vinden tussen het inperken van het recht op vrije meningsuiting en de strijd tegen schadelijke inhoud. Gesterkt door de *Code of Conduct on Disinformation*¹⁰⁷ van de Europese Commissie, omvatten deze initiatieven bijvoorbeeld het toekennen van labels aan online inhoud (*flagging*), het opleggen van verificatievereisten aan gebruikers, het toepassen van *factchecking*-procedures, of het aanbrenge van corrigerende notities (*community notes*) bij misleidende socialemediaberichten.¹⁰⁸ Daarbovenop biedt het gebruik van steeds geavanceerdere moderatietools ook nieuwe mogelijkheden, zoals het *downranken* van inhoud (waarbij het platform minder zichtbaarheid geeft aan bepaalde inhoud) en het *shadowbannen* van gebruikers (waarbij het platform de inhoud van een gebruiker eigenlijk verborgen houdt zonder de gebruiker daarvan op de hoogte te brengen).¹⁰⁹ In beide gevallen gaat het dus over manieren om het engagement (*likes, shares, comments*) met de schadelijke inhoud te laten dalen, zonder de inhoud als dusdanig te verwijderen. Hoewel dit langs de ene kant methodes zijn om de algemene voorwaarden van het platform te handhaven en schadelijke inhoud te beperken, moet er tegelijk worden erkend dat dergelijke technieken ook een zekere mate van controversie aanwakkeren. Zo zou het onlineplatform diezelfde technieken eveneens kunnen aanwenden om bepaalde politieke standpunten meer of juist minder zichtbaarheid te geven. Uit de transparantierapportageverplichtingen van verschillende VLOP's volgt overigens dat dergelijke bezorgdheden niet geheel onterecht zijn, met meldingen van geautomatiseerde contentmoderatiesystemen die gemiddeld zo'n 8,0-14,4% van geplaatste inhoud als valspositief aanduiden.¹¹⁰ Voor specifieke talen waar er minder trainingsdata voorhanden zijn, ligt dit foutenpercentage bovendien aanzienlijk hoger.¹¹¹ Uit het transparantierapport van Pinterest valt ook op te merken dat het foutenpercentage van hun contentmoderatiesysteem opvallend hoger ligt bij het detecteren van samenzweringstheorieën, misinformatie, en intimidatie.¹¹² Als reactie hierop valt ook op te merken dat, vanuit de kant van gebruikers van onlineplatforms, een fenomeen opduikt waarbij gebruikers de (mogelijk te strenge) contentmoderatiesystemen trachten te omzeilen. Het begrip

103 Reuters, 'Meta fixes error that flooded Instagram Reels with violent videos' (Reuters, 27 februari 2025) <<https://www.reuters.com/technology/meta-fixes-error-that-flooded-instagram-reels-with-violent-videos-2025-02-27/>> geraadpleegd op 5 maart 2025.

104 Zo spreekt Andrea Palumbo, 'A Medley of Public and Private Power in DSA Content Moderation for Harmful but Legal Content: An Account of Transparency, Accountability and Redress Challenges' (2024) 15 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 246, 250-251 over “harmful but legal content”.

105 Artikel 3(h), DSA definieert ‘illegale inhoud’ als volgt: “alle informatie die op zichzelf of in verband met een activiteit, waaronder de verkoop van producten of het aanbieden van diensten, indruist tegen het Unierecht of tegen het met het Unierecht in overeenstemming zijnde recht van een lidstaat, ongeacht het precieze voorwerp of de precieze aard van dat recht”.

106 Wat de sanctiemogelijkheden van de DSA betreft, zie artikel 52, DSA.

107 Europese Commissie, *Code of Conduct on Disinformation* (Publications Office of the European Union 2025) 49 p.

108 *Ibid.*

109 Wat betreft *downranking* en *shadowbanning*, zie rechtsoverweging 55, DSA.

110 LinkedIn ‘Digital Services Act Transparency Report’ (2023) Transparency report 1, 12.

111 *Ibid.*

112 Pinterest, ‘Digital Services Act Transparency Report’ (Pinterest, 11 oktober 2024) <<https://policy.pinterest.com/en/digital-services-act-transparency-report>> geraadpleegd op 20 februari 2025.

algospeak duikt in deze context regelmatig op om te verwijzen naar het fenomeen waarbij gebruikers op zoek gaan naar nieuwe codewoorden of andere, meer veilige formuleringen om te voorkomen dat contentmoderatiefilters inhoud zouden censureren.¹¹³ Zo worden sommige woorden afgekort (bv. SA voor “sexual assault”)¹¹⁴ of duikt de Engelse frase “to unalive oneself” op om contentmoderatiefilters (waarbij “to commit suicide” wordt gecensureerd) te ontlopen.¹¹⁵ Het onderliggend gegeven hierbij is dat algoritmes inhoud aanduiden als ongepast of niet wenselijk wanneer er bepaalde woorden worden vermeld, met als resultaat dat gebruikers actief op zoek gaan naar manieren om dezelfde boodschap te brengen op een andere manier.

Het zal ook in de toekomst een delicate kwestie blijven om een goede balans te vinden tussen contentmoderatie enerzijds en het recht op vrije meningsuiting binnen de platformomgeving anderzijds. Mediaberichten uit 2025 brachten dit thema opnieuw onder de aandacht nadat Facebook overging tot het afschaffen van *factchecking* in de VS – terwijl het dit in de EU bleef handhaven – onder het mom van vrijheid van meningsuiting.¹¹⁶ Daarnaast kondigde Meta aan te willen overstappen op het systeem van de eerder vermelde *community notes*, zoals tegenwoordig reeds gebruikt wordt op X. Dit lijkt echter haaks te staan op het beleid van de DSA, dat zich richt op sterkere contentmoderatie: terwijl Meta de verantwoordelijkheid voor contentmoderatie wil verschuiven naar haar gebruikers, streeft de DSA ernaar om juist meer verantwoordelijkheid bij de zeer grote onlineplatforms te leggen.

Dergelijke beslissingen leggen in feite een dieper spanningsveld bloot: *in hoeverre moeten onlineplatforms ingrijpen in contentmoderatie en wanneer wordt zo'n ingrijpen gelijkgesteld met censuur?* Hoewel we in deze bijdrage het antwoord op deze vraag schuldig blijven, durven we wel te stellen dat als gevolg van dit spanningsveld er wellicht altijd een kat-en-muisspel zal bestaan tussen geautomatiseerde contentmoderatiesystemen en gebruikers die deze systemen proberen te omzeilen. Een belangrijke uitdaging binnen deze dynamiek is dat informatie over de werking van de contentmoderatiesystemen tot voor kort volledig binnen de platformomgeving verborgen bleef.¹¹⁷ De vereiste om transparant te zijn over het moderatiebeleid – bv. door relevante data te delen voor onafhankelijke onder-

zoeksdoeleinden¹¹⁸ – vormt bijgevolg een noodzakelijke stap om te kunnen oordelen of er daadwerkelijk een goed evenwicht bestaat tussen de vrijheid van meningsuiting en verantwoorde contentmoderatie.

4. Algoritmische transparantie binnen de DSA

4.1 Aanbevelingssystemen binnen de platformomgeving

In het verlengde van de verplichting om beperkingen aan het gebruik van de platformomgeving te signaleren via de algemene voorwaarden,¹¹⁹ volgt uit artikel 27 DSA dat onlineplatforms voorts duidelijkheid moeten scheppen omtrent het gebruik van hun aanbevelingssystemen: de *verplichting tot algoritmische transparantie*.¹²⁰ Indien dergelijke algoritmische systemen zijn geïmplementeerd binnen de platformomgeving, dan legt de DSA op dat de dienstverlener via de algemene voorwaarden duidelijk moet aangeven wat de voornaamste parameters zijn om inhoud aan te bevelen aan gebruikers, alsook dat de dienstverlener beargumenteert waarom bepaalde parameters voor een bepaalde gebruiker (relatief gezien) van belang zijn. Tot slot vereist artikel 27 DSA ook dat, wanneer er meerdere instellingen voorhanden zijn om inhoud te rangschikken – denk bijvoorbeeld aan een sortering van inhoud op basis van populariteit versus op chronologische volgorde – gebruikers over de mogelijkheid moeten beschikken om dergelijke voorkeursinstellingen eenvoudig aan te passen.

Een diepgaandere analyse van een aantal aanbevelingssystemen levert ons nuttige inzichten op wat de werking ervan betreft.¹²¹ Eén van de voornaamste bevindingen is dat de gebruikerservaring binnen een onlineplatform – de inhoud die wordt getoond aan de gebruiker – significant kan verschillen naargelang de gebruiker al dan niet een account op het platform heeft en ook effectief is ingelogd. Wat de invulling van nieuwsfeeds betreft, zal het niet verwonderen dat in eerste instantie inhoud wordt getoond van andere profielen waarop de gebruiker zich heeft ‘geabonneerd’ of die de gebruiker ‘volgt’. In aanvulling daarop krijgen gebruikers gewoonlijk ook inhoud te zien waarop ze niet zijn geabonneerd, maar die desalniettemin nauw aansluit bij de gekende interesses van de gebruikers: zogenaamde gerelateerde inhoud die het platform presenteert met het label “you might also like”.

¹¹³ Ella Steen, Kathryn Yurechko en Daniel Klug, ‘You Can (Not) Say What You Want: Using Algospeak to Contest and Evade Algorithmic Content Moderation on TikTok’ (2023) 9 Social Media + Society 1, 1-2.

¹¹⁴ *Ibid.*, 5.

¹¹⁵ *Ibid.*, 11.

¹¹⁶ Joel Kaplan, ‘More Speech and Fewer Mistakes’ (*Meta*, 7 januari 2025) <<https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/>> geraadpleegd op 21 februari 2025.

¹¹⁷ Zoals ook aangehaald door Niels Jak, ‘Big Tech vanuit democratisch rechtsstatelijk perspectief’ [2023] 2 *Computerrecht* 101, 103.

¹¹⁸ In die zin, zie bijvoorbeeld Beschluss des Landgericht Berlin II vom 2. Februar 2025, *Democracy Reporting International v. Twitter International Unlimited Company* [2025] 41 O 140/25 eV; Anupriya Datta, ‘Berlin court rules against X on data access’ (*Euractiv*, 7 februari 2025), <<https://www.euractiv.com/section/tech/news/berlin-court-rules-against-x-on-data-access/>> geraadpleegd op 20 februari 2025.

¹¹⁹ Cf. artikel 14, DSA.

¹²⁰ Zie eveneens rechtsoverweging 70, DSA.

¹²¹ Voor een duidelijk overzicht: X, ‘Reddit’s Approach to Content Recommendations’ (*Reddit*, 22 november 2024) <<https://support.reddithelp.com/hc/en-us/articles/23511859482388-Reddit-s-Approach-to-Content-Recommendations>> geraadpleegd op 21 februari 2025.

Naarmate de gebruiker meer tijd doorbrengt binnen de platformomgeving, wordt het mogelijk om de getoonde inhoud steeds meer te personaliseren. Typische parameters die daarvoor worden gehanteerd zijn in eerste instantie de *aard van de inhoud* zelf: het thema, het aantal likes van andere gebruikers op de inhoud, de commentaargeschiedenis, het type van de inhoud (bv. tekst, foto, of video), alsook de nieuwheid van de inhoud. Zo kan al snel het onderscheid worden gemaakt tussen een gebruiker die enkel passief naar de meest populaire content kijkt, of een meer actieve gebruiker die graag met verse content interageert en actief commentaren plaatst bij die inhoud. Daarnaast worden aanbevelingen in zeer grote mate afgestemd op de *activiteiten van de gebruiker* binnen de platformomgeving. Iemand die bijvoorbeeld consistent naar een bepaalde livestream kijkt, naar een wekelijkse podcast luistert, likes geeft aan een specifieke influencer, of inhoud over een bepaald thema opzoekt, zal die content ook hoger zien verschijnen in zijn of haar gepersonaliseerde content feed. Tot slot zijn er nog een reeks andere personalisatieparameters, zoals de *leeftijd van het account* en *locatievoorkeuren*. Het finale doel van de aanbevelingssystemen is om via voorspellende modellen proberen te anticiperen wat een gebruiker wel of juist niet zou willen zien; een proces dat dynamisch kan worden bijgestuurd aan de hand van de hogervermelde factoren.

4.2 Controle voor de gebruiker over getoonde inhoud

De verplichting om te voorzien in algoritmische transparantie is een logische stap om ervoor te zorgen dat gebruikers meer autonomie hebben over de inhoud die ze te zien krijgen binnen de platformomgeving. Onlineplatforms verlaten zich namelijk op aanbevelingssystemen om *user engagement* hoog te houden: hoe meer tijd een gebruiker op een platform doorbrengt en hoe vaker een gebruiker met een platform interageert, des te waardevoller dit is voor het platform. Die drijfveer resulteert uiteindelijk in een strijd voor de aandachtspanne van gebruikers, een strijd die wordt beslecht door allerlei algoritmische tools die inhoud zodanig samenstellen en prioriteren dat gebruikers zo lang als mogelijk actief blijven op het platform.

Vanuit dat inzicht is het mogelijk om een aantal recente trends – zoals de opkomst van zeer korte video's (*shorts*) – beter te begrijpen: gebruikers krijgen in kleine tijdspannes een dopaminehit en blijven daardoor geëngageerd binnen het platform. Dergelijk gedrag kan op zijn beurt aanleiding geven tot het fenomeen van *doomscrolling*, waarbij gebruikers op quasi dwangmatige wijze eindeloos en doeleloos inhoud blijven consumeren. De risico's die gepaard gaan met het ontwerpen van interfaces en het afstemmen van algoritmes op manieren om *user engagement* op te drijven, zijn niet onopgemerkt gebleven en gaven onder andere aanleiding tot een voorstel van een

groep Europarlementariërs om bepaalde platformfeatures te verbieden of in te perken.¹²²

Er is reeds uitgebreid onderzoek gevoerd naar de negatieve implicaties van algoritmische systemen binnen de platformomgeving, met name in de sociale wetenschappen.¹²³ Prominente aandacht gaat daarbij uit naar de nefaste impact op het *mentale welzijn van gebruikers*. Verslavende ontwerpelementen binnen de platformomgeving – zoals de mogelijkheid om oneindig te scrollen, *pull to refresh*-mechanismen, en het automatisch afspelen van video's – spelen in op de kwetsbaarheden van individuele gebruikers en stimuleren de gebruikers om meer tijd door te brengen op het platform. Van de gemiddelde gebruiker verwachten dat hij of zij dergelijke manipulatieve technieken kan weerstaan op basis van pure zelfdiscipline lijkt onrealistisch.

Daarnaast heeft een andere bezorgdheid betrekking op het ontstaan van *filterbubbles* en *echokamers*. Wanneer aanbevelingssystemen prioriteit geven aan engagement boven diversiteit qua inhoud, dan worden gebruikers ook in toenemende mate blootgesteld aan inhoud die hun bestaande opvattingen versterken, en waarbij tegelijkertijd minder zichtbaarheid wordt gegeven aan alternatieve standpunten. Vanuit het gegeven dat inflammatoire of provocerende inhoud een hoger engagement genereert, is het risico van het algoritmisch cureren van inhoud dat het dan ook bijdraagt aan een toenemende mate van maatschappelijke verdeeldheid.

Om deze problemen aan te pakken, is het vereist dat gebruikers meer controle krijgen over de rankingssystemen die hen inhoud aanbevelen. In die zin is – onzes inziens – de verplichting tot algoritmische transparantie op zichzelf bekeken niet genoeg, maar vormt het wel een noodzakelijke opstap om gebruikers beter te informeren én ook uit te rusten om aanbevelingssystemen aan te passen. Het is te hopen dat de optie om individuele instellingen te kiezen, kan bijdragen aan het verminderen van vooroordelen, het verkleinen van risico op manipulatie, en ook de cyclus kan doorbreken waarin gebruikers louter inhoud te zien krijgen die hun wereldbeeld verengt.

4.3 Algoritmische transparantie volgens de Europese Commissie

Uit een gecombineerde lezing van de voorgaande secties volgt dat de DSA een duidelijke verplichting oplegt aan VLOP's en VLOSE's om de impact van algoritmische con-

122 Europees Parlement, Addictive design of online services and consumer protection in the EU single market [2023] 2023/2043(INI) final compromise amendments 1-22; Europees Parlement, 'New EU rules needed to make digital platforms less addictive' (25 oktober 2023) <<https://www.europarl.europa.eu/news/en/press-room/20231023IPR08161/new-eu-rules-needed-to-make-digital-platforms-less-addictive>> geraadpleegd op 20 februari 2025.

123 Bijvoorbeeld: Engin Bozdogan en Jeroen van den Hoven, 'Breaking the Filter Bubble: Democracy and Design' (2015) 17 Ethics and Information Technology 249; Florian Saurwein en Charlotte Spencer-Smith, 'Automated Trouble: The Role of Algorithmic Selection in Harms on Social Media Platforms' (2021) 9 Media and Communication 222.

tentcuratie en, bij uitbreiding, systeemrisico's voor de maatschappij tot een minimum te beperken. Echter, ondanks de geldende verplichtingen wijzen verscheidene lopende procedures van de Europese Commissie op aanhoudende problemen hieromtrent.

4.3.1 *Meta*

Een eerste voorbeeld zien we bij Meta, de aanbieder van Facebook en Instagram, waartegen de Europese Commissie in 2023 een formele procedure opstartte.¹²⁴ Als VLOP's moesten Facebook en Instagram vier maanden na het ontvangen van hun aanwijzingsbesluit¹²⁵ voldoen aan de verplichtingen die zijn opgenomen in artikels 33-43 van de DSA. Echter, uit het risicobeoordelingsrapport dat Meta in september 2023 heeft opgesteld, bleek dat niet aan alle verplichtingen was voldaan.¹²⁶ De vermeende inbreuken die de EC beide platformen ten laste legt, hebben betrekking op vier verschillende facetten.¹²⁷

Ten eerste zou Meta niet voldoen aan de verplichtingen m.b.t. de verspreiding van misleidende advertenties en desinformatie binnen de EU, zijnde het bieden van transparantie over hun advertentie-algoritmen. Een gebrek aan inzicht in hoe deze algoritmische systemen gebruikersinhoud prioriteren kan immers risico's opleveren voor de consumentenbescherming, het maatschappelijk debat en verkiezingsprocessen.

Ten tweede lijkt hun benadering tegenover politieke inhoud – waarbij dergelijke inhoud minder zichtbaar wordt gemaakt door middel van aanbevelingssystemen – onverenigbaar met de toepasselijke transparantieplichtingen en met de eis om systeemrisico's voor het maatschappelijk debat en verkiezingen te beperken. Wat dit betreft, haalt de Europese Commissie aan dat de niet-naleving van de transparantieplichtingen het voor gebruikers moeilijk maakt om te begrijpen hoe politieke inhoud op een betrouwbare manier wordt weergegeven.

Ten derde heeft Meta geen passend alternatief geboden voor de geplande stopzetting van CrowdTangle, hun instrument voor het real-time monitoren van het maatschappelijk debat en verkiezingsinmenging. Dit brengt systeemrisico's met zich mee, zoals de onmogelijkheid om desinformatie of kiezersonderdrukking op te sporen evenals het wegvallen van real-time transparantie voor factcheckers, journalisten en andere stakeholders omtrent degelijke inhoud. Voorts maakt dit het ook moeilijker voor onderzoekers om toegang

te krijgen tot data om de werking van algoritmische systemen van de twee platforms te bestuderen.

Ten vierde blijkt dat het kennisgevings- en actiemechanisme om illegale inhoud te melden niet in overeenstemming is met de verplichtingen van de DSA omtrent toegankelijkheid en gebruiksvriendelijkheid, en wordt Meta ten laste gelegd om geen doeltreffend intern klachtenafhandelingsysteem te hebben geïmplementeerd.

4.3.2 *AliExpress*

Ook tegen onlineplatform AliExpress, met maandelijks 104,3 miljoen actieve gebruikers in de EU en daardoor tevens een VLOP, werd eerder door de Commissie een procedure ingeleid voor een reeks vermeende inbreuken op de DSA.¹²⁸ Hoewel de EC verschillende elementen naar voren brengt, zijn er drie componenten die de aandacht verdienen.

Vooreerst gaat het over de naleving van de verplichting om systeemrisico's te beoordelen en te beperken,¹²⁹ zoals de verspreiding van illegale inhoud, opzettelijke manipulatie met verborgen links, en risico's omtrent influencers die schadelijke producten promoten.¹³⁰

Verder heeft de procedure ook betrekking op de verplichting om de betrouwbaarheid en volledigheid van de informatie die wordt gevraagd aan handelaren te beoordelen,¹³¹ de verplichting om transparantie te bieden over de belangrijkste parameters in de aanbevelingssystemen,¹³² en te voorzien in minstens één optie voor aanbevelingssystemen die niet is gebaseerd op profilering.¹³³ Hier niet aan voldoen beperkt immers de keuzevrijheid van de consument, alsook de mogelijkheid om de identiteit en betrouwbaarheid van handelaars na te gaan.

Daarnaast gaat het ook over de verplichting om te voorzien in een doorzoekbaar en betrouwbaar register voor advertenties.¹³⁴ Het ontbreken van een dergelijk register creëert immers een extra barrière voor consumenten om de algoritmische beslissingen achter getoonde advertenties te kunnen begrijpen.

4.4 *Bredere kijk op algoritmische transparantie*

De twee hogervermelde procedures – evenals de andere lopende DSA-procedures – onderstrepen niet alleen het belang van algoritmische transparantie, maar ook de uitdagingen gekoppeld aan de afdwinging ervan. Commissievoorzitter Ursula von der Leyen benadrukte dat vooral in tijden van democratische verkiezingen de EC optreedt

124 Europese Commissie, 'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram' (*Europese Commissie*, 16 mei 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664> geraadpleegd op 19 februari 2025.

125 Dit stemt overeen met eind augustus 2023.

126 Facebook, 'Systemic Risk Assessment and Mitigation Report for Facebook' (2024) Risk assessment report 1, 17 *et seq.*

127 Europese Commissie, 'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram' (*Europese Commissie*, 16 mei 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664> geraadpleegd op 19 februari 2025.

128 Europese Commissie, 'Commission opens formal proceedings against AliExpress under the Digital Services Act' (*Europese Commissie*, 14 mei 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1485> geraadpleegd op 19 februari 2025.

129 Zie hoger bij 2.3.3 *Risicobeoordelingen en risicobeperkingen*.

130 Europese Commissie, 'Commission opens formal proceedings against AliExpress under the Digital Services Act' (*Europese Commissie*, 14 mei 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1485> geraadpleegd op 19 februari 2025.

131 Artikel 30, DSA.

132 Artikel 27, DSA.

133 Artikel 38, DSA.

134 Artikel 39, DSA.

wanneer er vermoedens zijn dat derde landen de regels tegen gerichte desinformatie en misinformatie schenden.¹³⁵ Digitale platforms moeten voldoende middelen beschikbaar stellen om te voldoen aan hun verplichtingen zodat de democratische waarden beschermd blijven. Doen zij dat niet, dan kan de EC een procedure inleiden met betrekking tot deze inbreuken; procedures die uiteindelijk kunnen resulteren in boetes die oplopen tot 6% van de wereldwijde omzet van de betrokken tussenhandeldiensten.¹³⁶

De algoritmische transparantieplichtingen van de DSA sluiten daardoor aan bij bredere Europese wetgevingsinitiatieven op het gebied van platformregulering en consumentenbescherming. De verplichting om aanbevelingssystemen transparanter te maken vormt een stap vooruit wat betreft de bescherming van gebruikers en het tegengaan van misleidende praktijken. Transparantie alleen is echter geen garantie voor eerlijkheid. Zelfs wanneer gebruikers begrijpen hoe algoritmes werken, kunnen platforms nog steeds oneerlijke praktijken hanteren. Bovendien blijft er twijfel in hoeverre platforms zich in de praktijk aan deze regels zullen houden. Ondanks strenge handhaving door de EC, blijkt uit bovenstaande voorbeelden dat ondernemingen nog steeds manieren vinden om de werking van hun algoritmes vaag te houden met onduidelijke of complexe parameterbeschrijvingen. Daarom is de DSA slechts één onderdeel van een breder juridisch kader voor algoritmische transparantie: een effectieve naleving van transparantieplichtingen vereist een combinatie van de DSA met andere wetgevende instrumenten, zoals de AI Act en de Algemene Verordening Gegevensbescherming (AVG). Op die manier kan het gebruik van algoritmische aanbevelingssystemen niet alleen transparanter worden, maar vooral ook eerlijker.

5. Slotbeschouwingen

Deze bijdrage beoogde om een overzicht te bieden van de voornaamste ontwikkelingen één jaar na de inwerkingtreding van de DSA. Anno 2025 is de conclusie dat de EC een proactieve houding heeft aangenomen wat betreft de afdwining van de DSA. Vooreerst gaat het over het uitvaardigen van 25 aanwijzingsbesluiten, op basis waarvan een reeks onlineplatforms en onlinezoekmachines het label van VLOP en VLOSE kregen toegeschreven. Daarnaast is het noemenswaardig dat de EC in de periode na de inwerkingtreding verschillende aangeduide VLOP's en VLOSE's confronteerde met verzoeken om informatie te verstrekken aan de EC.¹³⁷ In 10 gevallen gaf dit uiteindelijk aanleiding tot het opstarten van een formele procedure om de dienstverlener te verplichten de DSA correct na te leven.

Tot slot moet ook worden opgemerkt dat de EC een aantal richtsnoeren en gedelegeerde verordeningen heeft gepubliceerd om meer duidelijk te bieden hoe bepaalde verplichtingen van de DSA moeten worden opgevat.

Daarnaast moet ook worden aangestipt dat de tussen dienstverleners zelf aanzienlijke stappen hebben ondernomen om gevolg te geven aan de DSA. Nu we één jaar verder zijn, zijn ook de transparantierapporten, informatie over het maandelijks aantal actieve gebruikers, de risicobeoordelingsrapporten van VLOP's en VLOSE's, evenals de onafhankelijke auditrapporten van deze entiteiten beschikbaar. Die documenten bieden een schat aan informatie voor onderzoek en het beter in kaart brengen van de werking van de platformomgeving. Een voornaam element hierbinnen is bijvoorbeeld de enorme schaal waarop de dienstverleners zich steunen op geautomatiseerde contentmoderatie, maar dat er ook een significant deel aan door gebruikers geplaatste inhoud valspositief als illegale inhoud wordt aangemerkt.

Als we verder uitzoomen en een breder perspectief hantieren, is het vooreerst correct om te stellen dat de DSA geen volledig nieuw instrument is, maar dat er voortgeborduurd wordt op eerdere aansprakelijkheids- en transparantieregels die terug te vinden zijn in de Richtlijn Elektronische Handel alsook de Richtlijn Consumentenrechten. De verplichting om illegale inhoud te verwijderen was ook reeds verankerd in instrumenten zoals de Verordening Terroristische Inhoud en Richtlijn 2011/92/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen. Toch neemt de DSA een grote stap vooruit wat betreft de bescherming van gebruikers (en hun fundamentele rechten) in de onlineomgeving, voornamelijk door de invoering van een geharmoniseerde aanpak tegenover illegale inhoud, naast een reeks bijkomende verplichtingen voor VLOP's en VLOSE's.

Toch blijven er ook nog verschillende open vragen. In eerste instantie gaat het over inhoudelijke vragen over de verordening zelf, zoals discussies over de draagwijdte van het criterium “verspreiding bij het publiek” dat de DSA hanteert om onlineplatforms te identificeren, of over de exacte berekeningswijze van het maandelijks aantal actieve gebruikers. In tweede instantie verdient het thema van de wisselwerking tussen de DSA en andere Europese instrumenten verdere aandacht in de toekomst. Hoger werd reeds opgemerkt dat algoritmische transparantie bijvoorbeeld een element is dat ook kan worden teruggevonden in de AI Act en de GDPR. Daarnaast is het ook duidelijk dat de DSA aansluiting zoekt bij de bestaande instrumenten van consumentenbescherming. Hoe de interacties tussen deze instrumenten concreet zullen moeten plaatsvinden, zal het onderwerp moeten zijn van toekomstig onderzoek.

¹³⁵ Europese Commissie, ‘Commission opens formal proceedings against TikTok on election risks under the Digital Services Act’ (*Europese Commissie*, 17 december 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487> geraadpleegd op 19 februari 2025.

¹³⁶ Artikel 52, DSA.

¹³⁷ Artikel 67, DSA.