NVPI – Position Paper inzake de Digital Services Act (DSA)[1]

1. Inleiding

NVPI is de Nederlandse brancheorganisatie van de entertainmentindustrie, met als leden platenmaatschappijen en filmdistributeurs.

NVPI verwelkomt het voornemen van de Commissie om middels het DSA-voorstel de verantwoordelijkheden van digitale diensten te verduidelijken, uit te breiden en te harmoniseren.

Sinds de inwerkingtreding van de Richtlijn inzake elektronische handel[2] uit het jaar 2000, is het aanbod van digitale diensten exponentieel toegenomen. Daar het DSA-voorstel een horizontaal karakter heeft en dus meerdere gebieden bestrijkt, is het van belang ervoor te waken dat **de voorgestelde bepalingen de bestaande situatie voor rechthebbenden niet verslechtert, zoals op het gebied van handhaving van auteursrechten en naburige rechten.** In dat verband stelt Overweging 11 van het DSA-voorstel terecht dat het voorstel "*geen afbreuk doet aan de regels van het Unierecht inzake het auteursrecht en de daaraan verbonden rechten, die specifieke regels en procedures vaststellen die onverlet moeten blijven*".

Wij zijn het met Europese Commissie eens dat het belangrijk is om het regime van de Richtlijn inzake elektronische handel te behouden. Ook in dat verband is het van belang dat het DSA-voorstel **niet leidt tot interpretaties of benaderingen die onbedoeld het huidige regime van aansprakelijkheid zouden (kunnen) verzwakken**.

2. Behoud toepassingsbereik en voorkom verzwakking van het aansprakelijkheidsregime

- *Behoud toepassingsbereik aansprakelijkheidsregime*
  Het is van belang dat er geen verruiming plaatsvindt van toepasselijkheid van de "*safe harbour*"-bepalingen van artikelen 12 tot en met 14 van de Richtlijn inzake elektronische handel. Daarvan zou sprake zijn indien een hogere drempel wordt gehanteerd voor de kwalificatie van een "*actieve rol*" van een digitale dienst. Hoewel het DSA-voorstel dezelfde categorieën "safe harbours" hanteert als de Richtlijn inzake elektronische

[1] Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende een eengemaakte markt voor digitale diensten (wet inzake digitale diensten) en tot wijziging van Richtlijn 2000/31/EG, Brussel, 15.12.2020, COM(2020) 825 final, 2020/0361 (COD).
[2] 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")

handel (caching, doorgifte en hosting)[3], zou in Overweging 18 van het DSA-voorstel mogelijk een hogere drempel kunnen worden gelezen ten aanzien van de kwalificatie van een "*actieve rol*". Dit zou echter in strijd zijn met het EU-acquis[4] (waaronder met name de uitspraak inzake *L'Oreal vs eBay*), en zou ingaan tegen het doel van het DSA-voorstel dat het bestaande aansprakelijkheidsregime gehandhaafd blijft. Een hogere drempel zou leiden tot minder verantwoordelijkheid voor digitale diensten, in plaats van juist meer. **Het is van belang dat elke verduidelijking ten aanzien van "*technische, automatische en passieve*" tussenpersonen en die welke een "*actieve rol*" spelen, strikt in overeenstemming is met het bestaande EU-acquis, teneinde te voorkomen dat de toepassing van "*safe harbours*" wordt verruimd**. De gekozen voorbeelden in de laatste zin van Overweging 18 zijn in dat verband ongelukkig omdat dat onbedoeld een hoge drempel zou kunnen suggereren voor het spelen van een "*actieve rol*" met als gevolg een ruimere toepassing van "*safe harbours*". **Het is belangrijk dat waar het DSA-voorstel voorbeelden noemt, dat voorbeelden uit de jurisprudentie van het Europese Hof van Justitie zijn, met name de uitspraak 'Oréal vs eBay (C-324/09)**. Daarin bepaalde de (Grote Kamer van) het Hof dat er sprake is van een actieve rol: "*wanneer hij bijstand verleent die onder meer bestaat in het optimaliseren van de wijze waarop de betrokken verkoopaanbiedingen worden getoond of het bevorderen daarvan".* Zie Overweging 45, punt 6 (Verklaring voor recht).

Voorkom verzwakking aansprakelijkheidsregime

Zodra een digitale dienst voldoet aan bovenbedoelde criteria (een technische, automatische en passieve rol), moet de dienst voldoen aan de nadere voorwaarden om in aanmerking te komen voor een "*safe harbour*". Het is van belang dat deze voorwaarden niet worden afgezwakt. Een cruciale voorwaarde met betrekking tot hosting providers, die in artikel 14 van de Richtlijn inzake elektronische handel is opgenomen, is dat de dienstverlener "*niet daadwerkelijk kennis heeft van de onwettige activiteit of informatie*" en, voor wat betreft een schadevergoedingsvordering, "*geen kennis heeft van feiten of omstandigheden waaruit het onwettige karakter van de activiteiten of informatie duidelijk blijkt*". Het eerstbedoelde "*daadwerkelijk kennis hebben*" is een andere norm dan de laatstbedoelde "*constructieve kennis*" (het "*besef*"). Constructieve kennis is ruimer dan daadwerkelijke kennis. Het is van belang dat deze begrippen niet door elkaar worden gehaald. Het DSA-voorstel lijkt deze normen te verwarren in Overweging 22. Dit zou de toepassing van de "*safe harbours*" kunnen verruimen, en daarmee in strijd zijn met de doelstellingen van de Commissie en nadelig zijn voor het voorkomen van verspreiding van illegale inhoud. **Wij stellen voor de verwijzingen naar "*besef*" ("*awareness*") te schrappen uit Overweging 22 van het DSA-voorstel, waarmee bedoelde verwarring wordt voorkomen**. Het is tevens belangrijk

[3] Hoofdstuk II, Artikel 3 t/m 5 DSA-voorstel.

[4] Google France cases (Joined cases C-236/08 to C-238/08), L'Oréal v eBay (C-324/09)

voor ogen te houden dat een kennisgeving of eigen onderzoek door de digitale dienst niet vereist is om daadwerkelijk kennis te hebben van illegale inhoud. Het kan bovendien zo zijn dat een kennisgeving aanleiding geeft tot kennis of besef van illegale inhoud of activiteit op een àndere plaats dan op de in een kennisgeving gespecificeerde URL('s).

- In Overweging 20 van het DSA-voorstel dient het woord "opzettelijk" te worden geschrapt. Er staat: "*Een aanbieder van tussenhandelsdiensten die opzettelijk met een afnemer van de diensten samenwerkt om illegale activiteiten te ontplooien, verricht zijn dienst niet neutraal en mag daarom niet in aanmerking komen voor de in deze verordening vastgestelde vrijstellingen van aansprakelijkheid*". **Opzettelijkheid is in de praktijk uiterst moeilijk te bewijzen en deze passage zou onzes inziens moeten worden geherformuleerd, zodanig dat deze ziet op alle digitale diensten die als hoofddoel hebben het verrichten of faciliteren van illegale activiteiten.**

- **De voorgestelde zorgvuldigheidsverplichtingen van het DSA-voorstel zouden voorwaarden dienen te zijn om in aanmerking te kunnen komen voor een "safe harbour**" daar het een extra incentive vormt voor de naleving van de zorgvuldigheidsverplichtingen, met name voor tussenpersonen die zich eventuele boetes voor niet-naleving kunnen veroorloven en deze als een kostenfactor verdisconteren.

- Het is een essentieel kenmerk van de aansprakelijkheidsregeling voor tussenpersonen in de Richtlijn inzake elektronische handel dat rechthebbenden of andere slachtoffers van illegale activiteiten een verbodsactie kunnen instellen tegen een tussenpersoon. Dit staat expliciet vermeld in artikel 12, 13 en 15 van de Richtlijn inzake elektronische handel. In Overweging 26 van het DSA-voorstel staat een formulering die verwarring kan veroorzaken. Er staat: "*Waar mogelijk moeten derden die te maken hebben met illegale inhoud die online wordt doorgegeven of opgeslagen, trachten conflicten met betrekking tot dergelijke inhoud op te lossen zonder de betrokken aanbieders van tussenhandelsdiensten daarbij te betrekken*". **Het is van groot belang dat dit wordt geschrapt en/of anderszins wordt verduidelijkt dat hiermee (en met de overige opmerkingen in Overweging 26) geen extra voorwaarde wordt gecreëerd voor (of anderszins afbreuk wordt gedaan aan) de mogelijkheid een verbodsvordering in te stellen.**

3. Flexibel en werkbaar mechanisme van kennisgeving

- De voorgestelde kennisgevings- en actiemechanismen zoals bedoeld in art. 14 DSA-voorstel moeten **meer flexibiliteit** bieden voor de verschillende soorten diensten en inhoud. Zo moet het mogelijk zijn een kennisgeving te doen ten aanzien van **diverse soorten inhoud en voor meerdere bestanden/materiaal waarop inbreuk wordt**

gemaakt. Er dient onzes inziens rekening te worden gehouden met het grote aantal inbreuken dat door rechthebbenden wordt gemeld[5].

- **Een verplichte vermelding van een URL (een adres van een bron op het internet), zoals bedoeld in art. 14 lid 2 sub b DSA-voorstel, zou moeten worden geschrapt.** Naast dat het een te zware last zou leggen op de melder om élk geval van dezelfde illegale inhoud te identificeren en te melden, is het niet effectief. Immers zouden hostingdiensten kunnen volstaan om alleen de URL te verwijderen, in plaats van alle inbreukmakende kopieën van hun servers te verwijderen. Ook geeft in sommige gevallen een URL geen nauwkeurige plaats aan van een specifieke inbreuk (bijvoorbeeld in een livestream of in een app).

- Art. 14 lid 6 DSA-voorstel bepaalt dat hostingdiensten na ontvangst van een kennisgeving deze op "*tijdige, zorgvuldige en objectieve wijze*" moet verwerken en daarover moet beslissen. Dit is niet in overeenstemming met de criteria die gelden om in aanmerking te komen voor de "*safe-harbour*" bedoeld in artikel 5 lid 1 sub b, namelijk: "*bij het verkrijgen van kennis of besef prompt handelt om de illegale inhoud te verwijderen of de toegang daartoe onmogelijk te maken*". **Prompt handelen dient de norm te zijn bij het verwerken van en het beslissen over een kennisgeving.**

- **Het DSA-voorstel zou de lidstaten de bevoegdheid moeten geven om versnelde procedures in te voeren waarbij dezelfde categorie digitale diensten dezelfde maatregelen moeten nemen met betrekking tot dezelfde inbreukmakende dienst.** Dit zou kunnen gebeuren in het kader van een nationale gerechtelijke procedure waarbij vonnissen uit andere EU-lidstaten worden gebruikt als basis voor het uitvaardigen van soortgelijke verbodsmaatregelen. In dit verband zouden ook de bepalingen inzake samenwerking tussen handhavingsinstanties verder kunnen worden ontwikkeld, bijvoorbeeld in art. 8 van het DSA-voorstel. Overigens lijken de artikelen 8 en 9 nodeloos in te grijpen in het recht van de lidstaten, bijvoorbeeld door aan rechterlijke uitspraken gestelde voorwaarden in de lidstaten. Het is van belang dat de toepassing van deze artikelen worden beperkt tot grensoverschrijdende uitspraken.

4. Verplichtingen moeten daadwerkelijk van betekenis zijn

Voor doeltreffendheid van de maatregelen om illegale inhoud te stoppen en te voorkomen, is het volgende van belang:

- **Verplichtingen dienen te worden opgelegd aan alle diensten die illegale content online mogelijk maken of faciliteren, ook indien of voor zover zij (mogelijk) niet**

[5] Ter illustratie: IFPI heeft sinds 2012 bijna 200 miljoen inbreuken gemeld op alle gecontroleerde platforms.

functioneren als "tussenhandelspersoon" ("intermediary service"), in de zin van art. 3 t/m 5 van het DSA-voorstel. Bijvoorbeeld domeinnaam registries/registrars, app stores, content delivery networks, payment providers en advertentienetwerken.

- **Verplichtingen ook voor micro- en kleine ondernemingen**[6]. Digitale diensten die in het kader van illegale inhoud worden gebruikt kunnen klein zijn en samenwerken met andere kleine partijen. In de praktijk komt het voor dat bij hostingdiensten gebruik wordt gemaakt van netwerken van kleinere ISP's. Ook is het gebruikelijk dat kleine partijen diensten en/of servers van grotere ISP's doorverkopen ("reselling"), en komt het voor dat inbreukmakende diensten servers huren om hun eigen (kleinere) ISP-dienst te exploiteren.

- **Een "*notice and stay down*"-verplichting dient te gelden voor hostingdiensten.** Een "*notice and takedown*" is niet effectief om rechthebbenden te beschermen[7]. Na ontvangst van een kennisgeving (en/of na het ontstaan van besef van inbreuken) zouden hostingdiensten verplicht moeten zijn om toegang tot al het aanbod van dezelfde inhoud te voorkomen en te verzekeren dat dezelfde inhoud niet nogmaals wordt aangeboden. Een "*stay down*" verplichting is noodzakelijk om effectief te zijn.

- **De "trusted flaggers" dienen daadwerkelijk voordelen te hebben van hun status en ook te gelden jegens micro- en kleine ondernemingen.** Onder meer door digitale diensten, inclusief micro- en kleine ondernemingen, te verplichten om aan meldingen van trusted flaggers onmiddellijk gevolg te geven, alsmede om -indien beschikbaar- gratis toegang te verlenen tot (technische) middelen om illegale inhoud op grote schaal te helpen opsporen (bijvoorbeeld middels een *Application Programming Interface ("API")*). Het is tevens belangrijk dat de opvolging van kennisgevingen afkomstig van anderen dan trusted flaggers niet verzwakt. **Het vereiste dat een trusted flagger "*collectieve belangen*"[8] dient te behartigen is ongerechtvaardigd en zou moeten worden geschrapt.**

- **Alle digitale diensten die illegale activiteiten mogelijk maken of faciliteren dienen een adequaat beleid te hebben inzake "*repeat infringers*" (herhaaldelijke inbreukmakers)**.
    - Dit dient ook te gelden voor micro- en kleine ondernemingen en niet alleen voor online platforms.

---

[6] Micro- of kleine ondernemingen in de zin van de bijlage bij Aanbeveling 2003/361/EG.
[7] Ter illustratie: in 2018 betrof 88% van de kennisgevingen van IFPI materiaal dat al eerder is gemeld aan dezelfde online dienst.
[8] Art. 19 lid 2 sub b en Overweging 46 van het DSA-voorstel.

- Bij de kwalificatie of iemand een repeat infringer is dient het te gaan om de **absolute hoeveelheid illegale content** en niet tevens de relatieve hoeveelheid zoals bedoeld in art. 20 lid 3 DSA-voorstel. Dit is van belang voor de effectiviteit en het bereiken van de doelstellingen van het DSA-voorstel.
- In dat verband dient ook de nadere voorwaarde **van "*manifest*" illegale inhoud, zoals genoemd in art. 20 lid 1 DSA-voorstel te worden geschrapt**.
- Ook dient te worden voorzien in mechanismen om te voorkomen dat repeat infringers zich, al dan niet onder een andere naam en/of account, **opnieuw laten registreren.**

- **Uitbreiden van de "Know Your Business Customer"-verplichting tot alle diensten van de informatiemaatschappij: niet alleen online-marktplaatsen (en inclusief micro- en kleine ondernemingen).** Hiermee biedt het DSA-voorstel de gelegenheid om de situatie te herstellen waarbij onrechtmatig handelende partijen de *Know Your Business Customer* verplichting, die reeds bestaat in art. 5 van de Richtlijn elektronische handel, in de praktijk straffeloos kunnen negeren. Zakelijke klanten hebben meer digitaal verkeer en betalen meer aan providers dan particuliere personen[9]. Met name in Nederland worden -naast veel legale diensten- veel illegale diensten gehost en gefaciliteerd. Zonder een *Know Your Business Customer* verplichting gaan dergelijke diensten ondanks een *Notice and Takedown (NTD)* eenvoudigweg gewoon verder. Het voldoen aan de verplichtingen is overigens gemakkelijker geworden doordat veel van die informatie al aanwezig en toegankelijk is dankzij de reeds bestaande registers die in het kader van de vijfde anti-witwasrichtlijn (2018/843/EU) van 30 mei 2018 tot stand zijn gekomen.

  Er dient te worden voorzien in een mechanisme om voor of namens belanghebbenden **tijdig toegang te krijgen tot die informatie** ten behoeve van onderzoek naar inbreukmakers en handhaving van rechten.

  Tevens is het van belang dat de informatie niet eenmalig bij aanvang wordt geverifieerd, maar ook meerdere malen (minstens jaarlijks) gedurende de tijd dat de gebruiker de diensten van de digitale dienstverlener ontvangt. Een dergelijke verplichting bevordert eveneens de bescherming van de consument tegen oplichtingswebsites, illegale goksites, sites met slechte of vervalste/schadelijke

[9] Een denkbare definitie zou bijvoorbeeld zijn: *"business customer": (a) legal entities, except any entity which qualifies as a large undertaking as defined in Article 3(4) of Directive 2013/34 of the European Parliament and the Council, or (b) any natural person that: (i) purchases a type or amount of service indicative of, or otherwise indicates, the intent to operate a business online; or (ii) contracts for the purchase of more than € 10,000 of services provided by the intermediary service provider in a one-year period, or (iii) is or becomes an information society service provider within the meaning of Directive (EC) 2000/31 of the European Parliament and of the Council*.

geneesmiddelen, malware etcetera. Dergelijke verplichtingen zijn gemakkelijk te implementeren door alle digitale diensten en met minimale administratieve last, zeker voor rechtmatige ondernemingen die immers hun zakelijke klanten reeds vragen zich te identificeren en eenvoudige controles daarop uitvoeren (op basis van openbaar beschikbare gegevens).

- **Het is van belang dat het DSA-voorstel een rechtsgrondslag bevat voor een openbaar WHOIS-register** dat minstens de gegevens bevat die reeds verplicht openbaar moeten worden gemaakt krachtens artikel 5 van de Richtlijn elektronische handel. Er dient een grondslag te zijn voor toegang tot WHOIS-informatie door belanghebbende personen of entiteiten voor het legitieme doel van onderzoek naar en de bestrijding van illegale activiteiten. Na inwerkingtreding van de GDPR is het WHOIS register in de praktijk echter vrijwel geheel ingetrokken, met grote nadelige gevolgen voor de mogelijkheden tot handhaving (gesprekken binnen ICANN leiden naar verwachting van belanghebbenden niet tot een werkbare oplossing).

- Het is van groot belang dat het DSA-voorstel blijft bevestigen dat het verbod op algemene toezichtverplichtingen **(a) niet uitsluit dat een dienst op eigen initiatief algemeen toezicht uitoefent, identificeert en inbreukmakende inhoud verwijdert en b) niet in de weg staat aan verplichtingen om specifiek toezicht uit te oefenen (zoals omschreven in overweging 28 van het DSA-voorstel).**

5. Bepaling vrijwillige maatregelen verduidelijken

Enerzijds zijn we het eens met de voorgestelde benadering in art. 6 van het DSA-voorstel om disincentives te voorkomen ten aanzien van het door digitale diensten proactief nemen van maatregelen inzake opsporen, identificeren en verwijderen van illegale inhoud. Anderzijds dient **verduidelijkt te worden dat deze bepaling alléén ziet op maatregelen die *uitsluitend* zien op het opsporen, identificeren en verwijderen van illegale inhoud (en de overige in het artikel genoemde maatregelen)**. Immers moet misbruik van de bepaling worden voorkomen, hetgeen in feite zou kunnen leiden tot een nieuwe "*safe harbour*". Voorkomen moet worden dat activiteiten die ook andere doelen hebben dan de vrijwillige proactieve maatregelen, automatisch buiten beschouwing zouden worden gelaten bij de beoordeling van de aansprakelijkheid van betreffende digitale dienst.

6. DSA-verplichtingen koppelen aan doeltreffende handhavingsmiddelen

Illegale websites opereren in heel Europa terwijl rechthebbenden per land actie moeten ondernemen op basis van rechtstelsels van de diverse landen. **Het is van belang dat benadeelde partijen toegang hebben tot effectieve handhavingsmechanismen in de gehele EU, zonder dat in elke afzonderlijke lidstaat een zaak moet worden aangespannen tegen dezelfde illegale dienst, dezelfde inbreukmakende activiteit of ten aanzien van dezelfde inbreukmakende**

inhoud. Het voorstel bevat geen bepaling met betrekking tot deze belangrijke problematiek. Dit is echter gewenst, zeker in verband met de DSA-doelstellingen. Tevens draagt het bij tot een oplossing voor de enorme werkdruk van rechterlijke instanties en bevordert het de goede werking van de interne vrije markt van de EU.

Daarnaast is het van belang dat naleving kan worden gehandhaafd ten aanzien van digitale diensten die niet in de EU zijn gevestigd.

Tevens zouden rechthebbenden een beroep moeten kunnen doen op maatregelen die betrekking hebben op **de volledige catalogus van de rechthebbende** (waarbij de inbreukmaker wordt verboden inbreuk te maken op alle beschermde inhoud van de eiser), en maatregelen die indien nodig op versnelde basis beschikbaar zijn.