

The Liability system of Art. 17 DSMD and national implementation

Contravening prohibition of general monitoring duties?

by **Gerald Spindler***

Abstract: The article deals with the complex liability system of Art. 17 DSM Directive, the famous “upload filter provision” in copyright law concerning content sharing platforms. The conflict between the prohibition of general monitoring obligations for platform providers derived from European fundamental rights by the CJEU and the obligations of providers are scrutinized. Moreover, possible options for national legislators in order to safeguard fundamental rights of users concerning freedom of speech (and copyright limitations) are discussed.

Keywords: Copyright liability; Service Provider; freedom of speech; copyright limitations; Upload-Filter; general monitoring obligations; European fundamental rights; flagging content; Art. 17 Digital Single Market Directive; user generated content; extended collective licenses

© 2019 Gerald Spindler

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Gerald Spindler, The Liability system of Art. 17 DSMD and national implementation – contravening prohibition of general monitoring duties? 10 (2019) JIPITEC 344 para 1.

A. Introduction

1 Scarcely any EU directive has attracted so much public attention as the new DSM-Directive,¹ which introduces obligations for service providers who enable sharing of user-generated content, such as

* Prof. Dr. Gerald Spindler is holder of the chair of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law and head of the Institute for Business Law at the University of Göttingen, Germany.

1 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, p. 92 ss. of 17.5.2019.

YouTube. The fight between rightholders on one side and the internet community on the other, fostered by large companies such as YouTube, even ended up in public manifestations against one article of the DSMD, Art. 17 (previously Art. 13). This article deals with obligations of service providers to control content on their platform, thus forming an exception of the safe harbor privileges for service providers enshrined in Art. 14 E-Commerce Directive.² It is obvious that such a control could hamper rights of freedom of speech as well as access to content – which is the legal ground for the claim filed by Poland against the DSMD and which lies

2 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178 p. 1 ss. of 17.7.2000.

at the core of the following article. I will initially shortly describe the existing system of copyright liability for intermediaries (B) before turning to the fundamentals of Art. 17 DSMD (C.1) whose structure is crucial for the constitutional analysis (C.3), in particular concerning the prohibition of general monitoring duties. Even if one does not follow the constitutional arguments, they have to be considered when implementing Art. 17 DSMD (D) which unfolded concerning user rights etc. Finally, we will discuss international private law implications (E), as well as the legal situation for those providers who are exempted from Art. 17 DSMD (F).

B. The Previous Liability System for Intermediaries

- 2 Originally, service providers – which also include operators of social networks or user-generated content platforms like YouTube – were covered without further question by the liability privilege of Art. 14 E-Commerce Directive; meaning that they could only be held liable after acquiring knowledge of any illegal content, or only if, “as regards claims for damages, (he) is not aware of facts or circumstances from which the illegal activity or information is apparent” (Art. 14 (1) sentence 1 (a) ECD) – which the courts applied to YouTube accordingly, freeing it from liability.³ However, in the *L’Oréal* decision, the CJEU made it clear that this privilege applies only to passive, neutral service providers, not to those who actively support users (e.g., through providing assistance and optimising the presentation of offers).⁴
- 3 From the beginning, injunctive reliefs on the grounds of liability for interference (“*Störerhaftung*”) have remained unaffected by the liability privilege – obligations which have in detail been formed by the jurisprudence in numerous decisions, but cannot be described here in detail. At its core, a host provider is liable as an interferer (“*Störer*”) after notification by the injured party regarding the future (!) omission of infringing rights if he violates reasonable inspection and control obligations (e.g. does not prevent that new content of the same kind is loaded onto the server).⁵ It should be noted, however, that even from a copyright perspective (up to now), the service provider itself does not commit any infringement in the sense that he is the offender or the infringer of an exploitation right of a copyright holder; at most he was a negligent side-perpetrator and therefore (apart from the liability for interference) could benefit from the liability privilege according to Art. 14 E-Commerce Directive.
- 4 However, this assessment changed with the development in CJEU case law on the right of making available to the public, Art. 3 a) InfoSoc Directive.⁶ With the decisions in *GS Media*, *Filmspeler* und *Pirate Bay*⁷ the CJEU already took the act of recovery far into the field of aid and its own actions.⁸ Specifically, it concerned hyperlinking (*GS Media*), a platform with piracy recommendations without hosting content (*Pirate Bay*), or hardware products with pre-set software that led to piracy platforms.
- 5 Whether the CJEU in the pending *YouTube*-proceeding⁹ would decide in the same manner is not agreed upon, since in this case – unlike *Filmspeler* and *Pirate Bay* – a targeted promotion of infringing acts of property rights by third parties cannot be concluded.¹⁰ Art. 17 (1) DSMD however, can be seen

EuZW 639, 640 ff.

3 Higher Regional Court Hamburg MMR 2016, 269; Higher Regional Court Munich CR 2016, 750.

4 CJEU Case C-324/09 *L’Oréal* EU:C:2011:474, para 116.

5 Further details in Spindler in Spindler/Schmitz (eds), *Telemediengesetz*, (2nd edn, CH Beck 2018), § 7 TMG paras 41 ff. with further proofs; see also Nico Gielen and Marten Tiessen, “Die neue Plattformhaftung nach der Richtlinie über das Urheberrecht im digitalen Binnenmarkt” [2019]

6 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167/10 ff.

7 CJEU Case C-160/15 *GS Media BV v Sanoma Media Netherlands* EU:C:2016:644, GRUR 2016, 1152 with comments by Ohly; CJEU Case C-527/15 *Filmspeler* EU:C:2017:300, GRUR 2017, 610 with comments by Neubauer/Soppe; CJEU Case C-610/15 *The Pirate Bay* EU:C:2017:456, GRUR 2017, 790; Matthias Leistner, “Die ‘The Pirate Bay’-Entscheidung des EuGH: ein Gerichtshof als Ersatzgesetzgeber” [2017] GRUR 755.

8 Rightly critical Leistner, (n 7) 755; Matthias Leistner, “Reformbedarf im materiellen Urheberrecht: Online-Plattformen und Aggregatoren” [2016] ZUM 580, 583; Matthias Leistner, “Anmerkung zu EuGH, Urteil vom 8. September 2016 – EUGH C-160/15” [2016] ZUM 980; CJEU Case C-160/15 *GS Media BV v Sanoma Media Netherlands* EU:C:2016:644, GRUR 2016, 1152, 1155 with comments by Ohly who speaks of a “substitute legislator”.

9 See the pending proceedings: Case C-682/18 *YouTube* and Case C-683/18 *Elsevier*; to the order for reference: Federal Court of Justice resolution of 13 September 2018 – I ZR 140/15, CR 2019, 100 ff.

10 Also the submitting Federal Court of Justice does not see an individual illegal action by platforms such as YouTube because of lack of knowledge and automation as given; Federal Court of Justice CR 2019, 100 para 30 ff. with

as a consequence of these decisions, provided that a general awareness of the platform provider is sufficient and a lack of neutrality¹¹ assumed.¹²

C. Compatibility of Art. 17 DSMD with the Primary European Law

I. System of Art. 17 DSMD

- 6 In order to verify the consistency of Art. 17 DSMD with the primary European Law¹³, first of all the system of Art. 17 DSMD with regard to the obligations of the provider (as defined by Art. 2 (6) DSMD [“online content-sharing service provider”])¹⁴ has to be explored in detail.

comments by Ohly; different opinion Malte Stieper, “Die Richtlinie über das Urheberrecht im digitalen Binnenmarkt” [2019] ZUM 211, 216 ff.

- 11 The CJEU had specifically emphasized this requirement with regard to Art. 14 of the E-Commerce Directive, CJEU Case C-324/09 L’Oréal EU:C:2011:474, CR 2011, 597 paras 113 ff.; CJEU Case C-236/08 *Google France SARL v Louis Vuitton Malletier SA*, CR 2010, 318 paras 114 ff.; in detail with further references Spindler (n 5) § 10 para 16, § 7 paras 8 ff., vor § 7 para 15; also Stephan Ott, “Das Neutralitätsgebot als Voraussetzung der Haftungsprivilegierung des Host-Providers” [2012] K&R 387 ff.; Matthias Leistner, “Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet” [2012] ZUM 722, 724 f.
- 12 Insofar too extensive Franz Hofmann, GRUR [2019] 1219, 1222 who believes that the liability now regulated in Art. 17 of the DSMD together with the “Stoererhaftung” (Breach of Duty of Care) already previously resulted in the responsibility of the platforms; Franz Hofmann, “Die Plattformverantwortlichkeit nach dem neuen europäischen Urheberrecht – »Much Ado About Nothing«?” [2019] ZUM 617, 623; similar Caroline Volkmann, “Art. 17 Urh-RL und die Upload-Filter: verschärfte Störerhaftung oder das Ende der Freiheit im Internet?” [2019] CR 376, 377 para 8.
- 13 Secondary European law must be ignored in this case, since the DSMD can displace other directives or regulations as lex posterior.
- 14 For simplification purposes, the term “service provider for sharing online content” is replaced in the following by the term “service provider”.

1. Definition of Service Providers for Sharing Online Content

a) Variety of Content in Organized Form

- 7 The service provider under Art. 2 (6) DSMD should be distinguished by the fact that at least “one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes”. Obviously it does not depend on the number of users themselves, but on the “large amount” of copyrighted works.¹⁵
- 8 Furthermore, the *content must be organised*; however this aspect is not specified precisely by the DSMD. It is probably sufficient if a search function for the search for certain content is maintained, as well as the creation of certain categories under which content can be found.¹⁶ Finally, the content must be “promoted” by the provider. Contrary to its ambiguous formulation, this provision should not be understood in a way that the provider promotes the concrete content (of the *user generated content*), rather that the provider offers an accompanying advertisement himself like YouTube does.¹⁷ Even news services that allow users to write comments (so-called “forum”) could be included in this definition, since wording is also protected by the copyright and per se under certain categories these are shared with many users and are often interconnected with advertisement.
- 9 Though services such as *Rapidshare*, which do not have search capabilities (hence, not organising content), or which do not place advertisements specifically within the content, are not covered by the DSMD, this is peculiar in terms of the number of copyright infringements to be found. However, Recital 62 DSMD considers this by explicitly mentioning at the end that “the exemption procedure under this Directive should not apply to service providers whose main purpose is to participate in or agree to facilitate copyright infringement.”

15 However, Recital 63 also refers to the public in order to specify Art. 2 (6) of the Directive.

16 Agreeing Nils Peters and Jan Henrik Schmidt, “Das Ringen um Upload-Filter geht in die 2. Runde” [2019] GRUR Int. 1006, 1006.

17 Agreeing Hofmann (n 12) 617, 628.

b) Negative Demarcation

- 10 Given the potentially large reach of the previous definition, Art. 2 no. 6 subsection 2 DSMD does make an effort to carve out certain services. In this context, the general criterion to be used can be Recital 62, which makes clear that no services should be affected:

“that have a main purpose other than that of enabling users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit from that activity”.

- 11 Accordingly, all non-commercial offers should be excluded – with a view to Wikipedia in particular – non-profit online encyclopedias but also scientific repositories. Similarly, platforms for open source software are excluded, including even commercial platforms such as “Online Marketplaces”. In view of the latter exception, it is decisive that any content other than *user-generated content* is essentially distributed for remuneration; because even here platforms for *user-generated content* are easily conceivable. The problems of demarcation further become apparent when the providers of electronic communications services according to the Directive 2018/1972¹⁸ are excluded (OTT-Services), which means that *WhatsApp* groups, as number-bound interpersonal communications services, are no longer covered by the DSMD¹⁹, even if they can fulfill the same functions when they are large enough as, for example, an account on Facebook in terms of sharing content.
- 12 What should not be underestimated regarding a teleological interpretation is the general line in Recital 62, which emphasizes that the scope of application:

“...should target only online services that play an important role on the online content market by competing with other online content services, such as online audio and video streaming services, for the same audiences”.

- 13 This could exclude from the scope many services that also use copyrighted content, such as dating and flirting portals with photographs and texts of their users.²⁰

18 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ L 321/36 ff.

19 Regarding the attribute as an OTT-Service: *Spindler* (n 5) § 1 para 26 ff.; Andreas Grünwald and Christoph Nüßling, “Kommunikation über die Top Regulierung für Skype, WhatsApp oder Gmail?” [2016] MMR 91, 92 f.

20 Accurately *Henrich*, <https://www.medienpolitik>.

c) Cloud-Services

- 14 Last but not least, “cloud services that allow users to upload content for their own use, are not online content-sharing service providers’ within the meaning of (the) Directive.” As reasonable as it may sound at first glance to exclude *GoogleDrive*, *MicrosoftOneDrive*, *iCloud*, etc. from the scope of application, a closer consideration reveals that there are considerable doubts. Since almost all cloud services allow the sharing of content, even the simultaneous editing of content. Services like *MicrosoftOneDrive* are actually designed to share content. How an effective demarcation shall be achieved here is difficult to assess; let alone a contract, stipulating that users are not allowed to share copyrighted content with others, is not sufficient. However, it is likely that cloud services are not captured by the framework of Art. 17 (1), since they rarely offer content to a large public (large numbers of people), so that an act of exploitation is missing per se.²¹

2. Independent Infringement of Exploitation Rights by Service Providers, Art. 17 (1) DSMD

- 15 The starting point of Art. 17 DSMD is the stipulation that the service provider within the meaning of Art. 2 (6) DSMD infringes the right of communication to the public according to Art. 3 (a) InfoSoc Directive, even if it concerns the content of third parties who uploaded them to the service provider platform (user-generated content). Thus, the activity of the service provider is not – as previously qualified in national law – a complicity or accessory act, but has to be seen as an independent violation of the rights of the copyright holder (own perpetrator).²² With good

[net/2019/04/plattformen-werden-verantwortung-uebernehmen/](https://www.net/2019/04/plattformen-werden-verantwortung-uebernehmen/), last accessed 17 April 2019; same opinion *Peters/Schmidt* (n 16) 1006, 1008.

21 Different opinion *Peters/Schmidt* (n 16) 1006, 1007, but without explaining where the necessary public should lie.

22 See also *Hofmann* (n 12) 1219; *Hofmann* (n 12) 617, 620 f.; *Arthur Wandtke and Ronny Hauck*, “Art. 17 DSM-Richtlinie – Ein neues Haftungssystem im Urheberrecht“ [2019] ZUM 627, 629; *Timm Pravemann*, “Art. 17 der Richtlinie zum Urheberrecht im digitalen Binnenmarkt – Eine Analyse der neuen europäischen Haftungsregelung für Diensteanbieter für das Teilen von Online-Inhalten“ [2019] GRUR 783, 784; *Volkman* (n 12) 376, 378 para 11; *Gielen/Tiessen* (n 5) 639, 642, however, with the hardly defensible assumption that then no further “*Stoererhaftung*” would apply – but this still exists due to the liability based on omission.

reason, doubt can be cast on the question of whether Art. 17 DSMD is a consistent implementation of the aforementioned CJEU case law (*GS Media, Filmpeleer, etc.*)²³ because of the non-specific intent to actually infringe the law - which in the end will be decided by the CJEU in the pending *YouTube* case.

- 16 According to the second subparagraph of Art. 17 (1) DSMD an online content service provider is required to obtain permission from the copyright holders referred to in Art. 3 (1) and (2) InfoSoc Directive, i.e. authors, performers, phonogram and film producers, as well as broadcasters. An extension of this consent requirement to other rights (ancillary rights) protected under national law, is not required by the Directive and does not seem necessary in view of the complexity of the provision. This is particularly important for platforms like Instagram which usually contain only amateur photos that are not protected by copyright.

3. Compulsory Program of the Service Provider

- 17 Art. 17 DSMD essentially stipulates two obligations of service providers within the meaning of the definition of Art. 2 (6) DSMD:
- primarily the obligation to obtain licences, Art. 17 (1), (4) (a) DSMD;
 - if this fails, the secondary obligation is to prevent the sharing of third-party content that violates copyrights, without further clarification of the measures required for this purpose, Art. 17 (4) (b) DSMD .
- 18 In addition, Art. 17 (4) (c) DSMD requires that copyright-infringing content of third parties that has been loaded onto the platform and has been notified to the provider is to be deleted by the provider, respectively blocked from access by third parties, and in the future to be restricted from again uploading it to the platform (notice-and-stay-down).²⁴

23 Doubtful by Leistner (n 8) 580, 586; agreed by Franz Hofmann, "Kontrolle oder nachlaufender Rechtsschutz – wohin bewegt sich das Urheberrecht? Rechtsdurchsetzung in der EU zwischen Kompensation und Bestrafung" [2018] GRUR 21, 28; Hofmann (n 12) 1218; Hofmann (n 12) 617, 620, 623 f.; Tobias Holzmüller, "Anmerkungen zur urheberrechtlichen Verantwortlichkeit strukturierter Content-Plattformen" [2017] ZUM 301, 302; Malte Stieper, "Ausschließlichkeitsrecht oder Vergütungsanspruch: Vergütungsmodelle bei Aufmerksamkeitsplattformen" [2017] ZUM 132, 137 f.

24 In detail Gerald Spindler, "Die neue Urheberrechtsrichtlinie

a) Obligation to Review Regarding Necessary Licences (Art. 17 (1), (4) (a) DSMD)

- 19 In other words, as a first step, the service provider needs to verify if content on its platform requires a license; in this case, he must then obtain the necessary licenses. The obligation of the service provider to obtain licenses - as he is generally considered as a possible infringer of the right of public access - leads initially to a general proactive investigation of the providers regarding their platforms, since otherwise - subject to Art. 17 (4) DSMD - they are responsible for copyright infringements.

- 20 Within this framework two sub-obligations have to be distinguished: the obligation to check any content for the possible necessity of licences (resp. copyright illegality); and the obligation to take care of this (!) determined content by obtaining the rights (license obtaining duty). For the obligation to check the content, it is decisive whether the service provider has to do this on his own initiative (pro actively) or only on the basis of information provided by the rightholder. Recital 66 seems to indicate that the service provider only has to act upon information received by rightholders. However, Recital 66 obviously refers to Art. 17 (4) (b) DSMD, which explicitly states that rightholders should provide the relevant information. Regarding the obligation to determine in the first place whether content subject to licensing is existent, Art. 17 (4) (b) DSMD does not appear to be relevant, since Art. 17 (4) DSMD provides for a staged liability: only if and when all efforts have been made to obtain licences - which necessarily implies that it was previously checked whether content subject to licence is actually existent - Art. 17 (4) (b) DSMD intervenes. In other words, Art. 17 (4) (b) DSMD is just one part of all obligations of the service provider and depends of compliance with obligations of Art. 17 (1), (4a) DSMD. Later we have to return again to this important distinction and system.

- 21 In order to obtain the licenses or permissions (Art. 17 (4) (a) DSMD) the service provider has to undertake serious efforts, be it with collecting societies or individual rightholders, in terms of getting in contact and a serious willingness to negotiate. On the other hand, it also does not matter whether the rightholder wishes to grant the rights for reasonable remuneration. There is no obligation to contract on the part of the copyright holder²⁵ nor on the part of

der EU, insbesondere <Upload Filter> - Bittersweet?" [2019] CR 277, 288; Hofmann (n 12) 617, 621 f.; also Gielen/Tiessen (n 5) 639, 646.

25 At the end of recital 61 of the DSMD it is specifically

the service provider²⁶ – notwithstanding antitrust considerations. Whether the Member State can foresee a contracting obligation by implementing Art. 17 seems rather doubtful in light of the DSMD.²⁷

- 22 However, the service provider does not have to carry out excessive research in order to identify a rightholder – for example in the case of orphan works – since here the principle of proportionality according to Art. 17 (5) DSMD also applies. Specific problems are posed by holders of copyrighted works that are not active in a professional manner, from amateur photographers to amateur videos, up to amateur authors. Corresponding licence offers will be missing in these cases; also, often enough it will be difficult for the service provider to determine the rights holder. Therefore, here too the service provider should not be targeted by overstretched obligations. Beyond collective licencing according to Art. 12 DSMD,²⁸ it should be sufficient that non-professional authors are offered a “monetization” by participating in the advertising revenue.²⁹ Service providers cannot rely any more solely on a presumed (or tacit) consent of the rightholder – as it has formerly been used as a justification by the Federal Court of Justice for the image search of Google;³⁰ this concept is not valid anymore, since the decision of the CJEU in *Renckhoff*-decision.³¹

mentioned that rightholders are not obliged to grant licenses.

- 26 In this regard, recital 64 of the DSMD only refers to the fact that service providers “should obtain” permission from rightholders, for instance by concluding a license agreement; as here Hofmann (n 12) 617, 620; hence *contra legem* Wandtke/Hauck (n 22) 627, 630, who speak of an obligation to conclude due to the efforts according to Art. 17 (4) a) DSMD.
- 27 As here Hofmann (n 12) 1223.
- 28 Thomas Dreier, “Die Schlacht ist geschlagen – ein Überblick” [2019] GRUR 771, 777 f. essentially focuses on this, but also recognizes the limits of this approach.
- 29 Accurately Hofmann (n 12)1226; even going beyond Grisse, “After the storm – examining the final version of Article 17 of the new Directive (EU) 2019/790”, [2019] JIPLP 887, 893.
- 30 Federal Court of Justice GRUR 2010, 628; critical on that matter Gerald Spindler, “Bildersuchmaschinen, Schranken und konkludente Einwilligung im Urheberrecht Besprechung der BGH-Entscheidung “Vorschaubilder” [2010] GRUR 785.
- 31 CJEU 2018 Case C-161/17 *Renckhoff* (Cordoba), EU:C:2018:634, GRUR 2018, 911.

- 23 The service provider is obliged to provide evidence of his readiness to negotiate and his search for rightholders, which requires appropriate documentation. In the best case, the licenses should be able to be queried automatically; however, the DSMD does not envisage any specific procedures here.³²
- 24 In this context, the principle of proportionality according to Art. 17 (5) DSMD is evoked in order to relativize Art. 17 (1) DSMD, respectively the obligations of the service provider in the sense of moderate due diligence, so that a comprehensive rights clearance *ex ante* is not required, since service providers, unlike traditional right users (press, media), do not have complete control of content.³³ As much as this may apply with regard to the acquisition of rights (i.e., the effort to obtain licences), this turns a blind eye to the fact that the requirements for obtaining any rights means first of all to check the content regarding any copyright infringement. Without controlling the complete content it cannot be clarified if or in which amount licenses must be obtained. A simple random check is not intended by the DSMD.
- 25 This argument also applies to a restriction of the obligation under Art. 17 (1) DSMD to an inspection only on the basis of prior notification by rightholders.³⁴ This is in clear contradiction to the system of Art. 17 (1), (4) (a) and (b) DSMD.³⁵

b) Duties and Responsibility Limitation by Art. 17 (4) (b) DSMD

- 26 In a second step, this liability is limited by Art. 17 (4) DSMD; the duties in para. 4 (a) – (c) have to be separated from those in Art. 17 (1) DSMD. The service provider has to show evidence that he has undertaken best efforts to obtain a license. Only if these efforts have failed, the service provider can turn to Art. 17 (4) b) DSM-Directive – which can certainly also be read as a kind of liability privilege. Since after (!) all unsuccessful efforts to obtain a licence, the service provider must monitor and verify that there is no content on its platform that infringes upon the rights of rightholders – but only
-
- 32 However, Art. 17 (10) merely provides for subsequent development of further guidelines on the application of Art. 17, in particular (4), by the Commission and the various stakeholders.
- 33 See Hofmann (n 12) 1224.
- 34 Still of this opinion Volkmann (n 12) 376, 378 para 24 ff.
- 35 See below D.III.1.

if the rightholders have provided the necessary information (Art. 17 (4) (b) DSMD). Without Art. 17 (4) (b) DSMD, the provider would principally be liable if he had not obtained a license for all relevant content. However, Art. 17 (4) (b) DSMD limits this liability as the efforts to be undertaken regard only the information provided by the rightholder. Recital 66 para 5 DSMD shows that the rightholders must actively provide this information.³⁶ That means vice versa: If the service provider does not have any information by the rightholder, he is not obliged to make any efforts according to Art. 17 (4) (b) DSMD.

- 27 In this case, the actual comprehensive obligation to investigate according to Art. 17 (1) DSMD is relativized for subsequent liability. Accordingly, Art. 17 (4) (b) DSMD can be qualified as an extension of the notice-and-stay-down obligation or the notice-and-take-down procedures according to Art. 14 ECD, more or less as an advance-protection.³⁷ Art. 17 (4) (b) DSMD would hereby correspond to a kind of early notification of all relevant content³⁸ – in contrast Art. 14 ECD demands notifying the provider of specific, incriminated content, so that the provider is able to then identify it on its platform.
- 28 Accordingly, it is inaccurate to locate the “upload filters” in Art. 17 (4) (b) DSMD that would exist independently (!) of rightholders’ information. Since the obligation in Art. 17 (4) (b) DSMD depends on this information by the rightholders and does not refer in general to all content on the platform, Art. 17 (4) (b) DSMD cannot be qualified as an obligation to check all content (and resulting in an “upload filter”). However, it should be clearly noted that this restriction in Art. 17 (4) (b) DSMD does not (!) apply at all to the previous obligation of Art. 17 (1), (4) a) DSMD to obtain licences; this obligation is clearly independent of any previous information by rightholders.
- 29 The Directive does not cite automatic procedures, but rather merely states in Art. 17 (4) (b) DSMD, that the service provider has to make all efforts “in accordance to high customary standards with all professional care”, in order to not make available the relevant user generated content. Conversely, the explicit requirement contained in Art. 17 (9) DSMD that the complaints of users should be examined by humans allows one to conclude that in all other cases an automated upload-filter is permitted, in particular regarding the possible measures according to Art. 17 (4) (b) DSMD.

36 Agreeing *Peters/Schmidt* (n 16) 1006, 1009.

37 *Pravemann* (n 22) 783, 786 rightly speaks of “Notice-and-prevent”-procedures; see *Wandtke/Hauck* (n 22) 627, 634.

38 See also *Hofmann* (n 12)1225.

How the high customary standards are to be determined and who participates in which process, are not further specified by the DSMD.

- 30 Further, the DSMD does not explain in which form the information is to be provided; certainly a machine readable information would make the most sense, but the service provider cannot demand such. The service provider does not have to examine the correctness of information provided by rightholders, so that any alleged copyright could be sufficient; counterclaims by affected persons (users) are not provided by the DSMD.³⁹

c) Notice-and-Stay-Down

- 31 In addition, Art. 17 (4) (c) DSMD provides the notice-and-take-down procedure, already known from the E-Commerce Directive, but explicitly adding the obligation to prevent a re-upload of the copyright infringing content in accordance with the standards of Art. 17 (4) (b) DSMD, thus again following the “high industry standards” (*stay-down*). However, the obligation is only triggered after “receiving a sufficiently substantiated notice from the rightholders”, thus apparently not in the case of information provided by a third party (in contrast to Art. 14 ECD)⁴⁰ but also not in the case of general information. The obligations are triggered regardless of whether the service provider has fulfilled his obligations under Art. 17 (4) (a) and (b), Recital 66 subpara. 6 DSMD.
- 32 From a German point of view, the obligation to keep the content “down” resembles much of the so-called “core theory” (“Kerntheorie”),⁴¹ which requires that

39 So far, such cases of abusive “notices” and information have been rarely discussed, in contrary to unjustified protection warnings, see more recently: Federal Court of Justice, GRUR 2016, 630 paras 15 ff.; for further details see Spindler in Gsell/et al. (eds) *Beck’scher Online Großkommentar* (CH Beck 2019), § 823 paras 220 ff. with further references.

40 See on this matter, Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final), chap. I no 4 (f), chap. II no 5-8, that identifies any natural person or entity as a notice provider.

41 On the subject “core theory”, see for instance Federal Court of Justice GRUR 2014, 706 with further proofs; Federal Court of Justice GRUR 2013, 370 paras 29 ff.; Federal Court of Justice GRUR 2011, 1038 para 39; Specht in Dreier/Schulze (eds), *Urhebergesetz* (6th edn, CH Beck 2018) § 97 paras 59, 67; on the application of core theory to image reporting, see recently Regional Court Frankfurt oM, ZUM 2019, 71, 72; Federal Court of Justice ZUM-RD 2009, 499 para 7 with

similar content should be blocked as well by the “stay-down” ban.⁴² The same approach was taken more or less already for Art. 14 ECD, however it was restricted to automatic controls.⁴³ The decision of the European Court of Justice on personal rights in the *Glawischnig-Piesczek* case now points towards a similar direction.⁴⁴ Since the service provider is obliged to prevent the upload of “synonymous” or similar content, the obligation of the notice-and-stay-down procedure is similar to the preventive procedure in Art. 17 (4) (b) DSMD, only with the difference that for Art. 17 (4) (c) DSMD, a specific message referring to an already stored content is necessary.

d) Principle of Proportionality

- 33 With regard to the efforts required by Art. 17 (4) (a) (c) DSMD, however, the principle of proportionality embedded in Art. 17 (5) DSMD also applies. Accordingly, with the:
- 34 “(Determination) whether the service provider has complied with its obligations under paragraph 4, and in light of the principle of proportionality, the following elements, among others, shall be taken into account:
- a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and
 - b) the availability of suitable and effective means and their cost for service providers.”
- 35 According to the perception of some authors,⁴⁵ small or young entrepreneurs should not be subject to the same standards as large companies; they should perhaps even be freed of the obligations of Art. 17
-
- further references.
- 42 See for instance Daniel Holznagel, “Schadensersatzhaftung gefahrgeneigter Hostprovider wegen nicht verhinderter “gleichartiger“ Inhalte” [2017] CR 463 ff.
- 43 See Spindler (n 5) § 7 paras 51 f. with further references; Holznagel/Höfingler in Hoeren/Sieber (eds), *Multimediarrecht* (44 edn, CH Beck 2017,) part 18.1 paras 56 ff.; Paal, § 7 TMG Rn. 65 in Gersdorf/Paal (eds), *BeckOK Informations- und Medienrecht*, (23 edn, CH Beck 2019).
- 44 CJEU Case C-18/18 *Glawischnig-Piesczek*, EU:C:2019:821; see on this matter *Spindler*, NJW 2019, 3274.
- 45 See e.g. Gielen/Tiessen (n 5) 639, 643 f.; similar Hofmann (n 12)1227.
- (4) (b) DSMD – unless other criteria counterbalance this, such as the type of works uploaded. However, this can hardly be reconciled with Art. 17 (6) DSMD, which provides for an exception for start-ups,⁴⁶ which was heavily controversial between Member States during the policy-making process and in the end codifies exemptions for small or younger entrepreneurs. Art. 17 (6) DSMD can not be put aside simply by applying the proportionality principle concerning small firms.
- 36 However, the relationship between Art. 17 (4) and (5) DSMD is not entirely clear either. Since in civil law (and therefore also in copyright law [beyond criminal copyright law]), objective standards of behavior are relevant,⁴⁷ it is open which role Art. 17 (5) DSMD shall play. There can be no question of determining an “individual accusation”, as this would foil the due diligence requirements. On the other hand, Art. 17 (5) DSMD does not explicitly state that these criteria should be taken into account when determining the standards, but rather “only” with regard to the question whether the service provider met the requirements, hence, more individually. Either the high customary standards, in favor of a case-by-case evaluation, are devalued or there is a kind of two-stage consideration, which – as already mentioned – does not correspond to the usual civil law dogmatics. Recital 66 subpara. 4 DSMD even states that “it cannot be ruled out that in some cases the availability of unauthorized content can only be avoided, if the rights holders have notified the provider”, in other words, no appropriate technologies are available that meet the criteria.
- 37 Finally, unlike the Art. 17 (4) DSMD, it is unclear who bears the burden of proof concerning the relevant factors: A general statement is not possible, since Art. 17 (5) DSMD can be both *exacerbating* (e.g. imposing higher obligations to service providers due to specific content or amount of content), as well as *relieving* (e.g. lowering obligations according to small amount of content or lacking financial resources). Depending on this, the corresponding burden of proof should be assigned to the concerned party.
-
- 46 Regarding this see below D.III.2.
- 47 See for instance Lorenz, § 276 paras 5, 20 f. in Bamberger/ et al. (eds), *Beck’scher Online Kommentar* (52nd edn, CH Beck 2019)) with further references; Schaub § 276, paras 72 ff. in Gsell/et al., *Beck’scher Online Großkommentar*, (CH Beck 2019); see also Spindler in Spindler/Schuster (eds), *Recht der elektronischen Medien* (4th edn, CH Beck 2019), § 97 para 19; Specht (n 41) § 97 para 58.

4. Limitations in Favor of Users

- 38 With regard to the limitations in favor of the users, Art. 17 (7) DSMD stipulates that users should, at any time be able to invoke in their favor the copyright limitations of citation, critic and review (Art. 17 (7) (a) DSMD), as well as use for the purpose of caricatures, parodies and pastiches (lit. b). The rights of users should be guaranteed by a complaint procedure, as laid down by Art. 17 (9) DSMD. Within the framework of the complaint procedure it is of importance that Art. 17 (9) DSMD envisages that:
- 39 “Complaints submitted under the mechanism provided for in the first subparagraph shall be processed without undue delay, and decisions to disable access to or remove uploaded content shall be subject to human review.”
- 40 Thereby, the DSMD attempts to balance between (automated) copyright protection on the one hand and a guarantee of limitations and freedom of expression on the other hand, especially with regard to the EU Charter of Fundamental Rights (Recital 70 DSMD). Thus, the measures are not intended to prevent copyright-free works or those subject to restrictions from being available.
- 41 Unfortunately, other limitations, such as the science and education limitation according to Art. 5 (3) (a) InfoSoc Directive are not mentioned so that they are not covered - which is difficult to understand, since Art. 17 DSMD refers only to copyrighted works so that all the limitations of Art. 5 of the InfoSoc Directive have to be applied (so far as they had been implemented by Member States) - and not only those mentioned in Art. 17 (7), even if these are the most relevant. If these limitations are applicable, the content is no longer subject to copyright infringement so that all obligations of Art. 17 DSMD would not apply either. However, the user cannot refer to them and enforce them, since Art. 17 (7), 9 DSMD lists only the mentioned limitations.

5. Ban of General Monitoring Obligations and its Relationship to the E-Commerce-RL

- 42 Art. 17 (8) DSMD then again explains that:

“The application of this Art. shall not lead to any general monitoring obligation.”

Furthermore, Art. 17 (3) DSMD determines the relationship to the liability privilege in Art. 14 ECD:

“When an online content-sharing service provider performs an act of communication to the public or an act of making

available to the public under the conditions laid down in this Directive, the limitation of liability established in Art. 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Art.

The first subparagraph of this paragraph shall not affect the possible application of Art. 14 (1) of Directive 2000/31/EC to those service providers for purposes falling outside the scope of this Directive.”

Whether this exclusion of the general monitoring obligations is sufficient under European Law, so that the constitutionally justified requirements of the European Court of Justice can be met, will be verified later.⁴⁸

6. Influence of the Stakeholder-Dialogue and Guidelines of the Commission to Art. 17 DSMD

- 43 Lastly, Art. 17 (10) DSMD stipulates the Commission to establish a dialogue with stakeholders – rightholders, service provider representatives, but also users’ organisations – in order to enable the Commission to develop guidelines for the design of the procedure under Art. 17 (4) DSMD for its further interpretation. In doing so *expressis verbis* the fundamental rights of the affected shall be taken into account.

II. Affected Fundamental Rights

- 44 From the described structure of Art. 17 DSMD, the affected fundamental rights within their multilateral relationship (user – service provider - rightholders - third-party users [content-retrieving users]) become clear:⁴⁹
- 45 First, the service providers are directly affected in their fundamental rights regarding the freedom to choose an occupation, respectively the freedom to conduct a business (Arts 15, 16), Art. 17 ECFR,⁵⁰ because the obligations imposed on them result in corresponding costs and burden their business models. It is not without reason that the EU legislator has introduced corresponding derogations for Start Ups, Art. 17 (6) DSMD, as well as a general proportional measurement in Art. 17 (5) DSMD, which also refers to the specific operation and scope of a platform.

48 See below C.III.

49 Similiar Hofmann (n 12) 617, 625 f.

50 Charter of Fundamental Rights of the European Union (2000/C 364/01), OJ C 364, p. 1 ss. of 18.12.2000

- 46 Furthermore, of course, the rights of users who upload content to the platforms are affected in their fundamental right to freedom of expression, Art. 11 ECFR. Furthermore, these users may also be affected in their data protection rights, Art. 8 ECFR, since the blocking of content may require the identification of the respective user.
- 47 However, even third users who do not upload content themselves but view or use content of other users are affected regarding their freedom of information (Art. 11 ECFR) because the content of others is not freely available. As the CJEU has already stated in the SABAM/Netlog decision⁵¹ and later (relating to access providers) in the decision UPC Telekabel,⁵² the rights of third parties are as well affected by such measures.
- 48 On the “opposite side”, fundamental rights of the rightholders from Art. 17 ECFR concerning the protection of property rights are affected, but also Art. 7 ECFR as a personality right as far as the actual authors are concerned (and not only right distributors).

III. The Ban of General Monitoring Obligations and Art. 17 DSMD

1. General Monitoring Obligations and the EU Charter of Fundamental Rights

a) Derivation from EU Fundamental Rights

- 49 Relevant and derived from the aforementioned fundamental rights is in particular the Netlog decision of the CJEU.⁵³ The case concerned a lawsuit of a Belgian collecting society against a service provider (social network) requiring it to proactively investigate all data transfers or activities for the purposes of copyright infringement.
- 50 In the Netlog decision the CJEU explicitly referred to the rights of freedom of expression and information, guaranteed in the EU Charter of Fundamental Rights in order to declare a general monitoring procedure, as demanded by the Belgian collecting company SABAM towards Netlog – a service provider – inadmissible. For the requested filter system, the CJEU initially stated:

“36 In that regard, it is common ground that implementation of that filtering system would require:

first, that the hosting service provider identify, within all of the files stored on its servers by all its service users, the files which are likely to contain works in respect of which holders of intellectual-property rights claim to hold rights;

next, that it determine which of those files are being stored and made available to the public unlawfully; and

lastly, that it prevent files that it considers to be unlawful from being made available.

37 Preventive monitoring of this kind would thus require active observation of files stored by users with the hosting service provider and would involve almost all of the information thus stored and all of the service users of that provider (see, by analogy, Scarlet Extended, paragraph 39).

38 In the light of the foregoing, it must be held that the injunction imposed on the hosting service provider requiring it to install the contested filtering system would oblige it to actively monitor almost all the data relating to all of its service users in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the hosting service provider to carry out general monitoring, something which is prohibited by Art. 15(1) of Directive 2000/31 (see, by analogy, Scarlet Extended, paragraph 40).”

- 51 These statements are of particular interest to the present question, since they show the proximity of the duties examined at that time to those of Art. 17 DSMD.
- 52 With regards to the fundamental rights concerned, the CJEU maintains – in continuation of the principles already outlined in the Promusicae decision – that the protection of intellectual property rights under Art. 17 (2) ECFR is not limitation-free and unconditionally guaranteed, i.e., a consideration regarding fundamental rights of other affected parties has to be made.⁵⁴ Accordingly the CJEU stresses in the Netlog decision:

“44 Accordingly, in circumstances such as those in the main proceedings, national authorities and courts must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as hosting service providers pursuant to Art. 16 of the Charter (see Scarlet Extended, paragraph 46).”

51 CJEU Case C-360/10 SABAM vs. Netlog, EU:C:2012:85.

52 CJEU Case C-314/12 UPC Telekabel, EU:C:2014:192.

53 CJEU Case C-360/10 SABAM vs. Netlog, EU:C:2012:85.

54 CJEU Case C-360/10 SABAM v Netlog, EU:C:2012:85, paras 41 f.; CJEU Case C-275/06 Promusicae, EU:C:2008:54, paras 62 – 68, esp. para 68; reaffirmed recently in CJEU Case C-516/17 Spiegel Online, EU:C:2019:625, paras 56 ff.

- 53 For the fundamental rights of service providers, the CJEU considers such an obligation to monitor general research, or to verify the content to be in violation of fundamental rights:

“46 Accordingly, such an injunction would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Art. 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly (see, by analogy, *Scarlet Extended*, paragraph 48).

47 In those circumstances, it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as hosting service providers (see, by analogy, *Scarlet Extended*, paragraph 49).”

- 54 But the CJEU does not only see the fundamental rights of the provider as disproportionately impaired, but also those of the users:

“48 Moreover, the effects of that injunction would not be limited to the hosting service provider, as the contested filtering system may also infringe the fundamental rights of that hosting service provider’s service users, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Art.s 8 and 11 of the Charter respectively.

49 Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified (see, by analogy, *Scarlet Extended*, paragraph 51).

50 Moreover, that injunction could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. In addition, in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned (see, by analogy, *Scarlet Extended*, paragraph 52).”⁵⁵

- 55 This interpretation of the ban of general monitoring obligations largely corresponds to the distinction between general and specific monitoring obligations already derived in Member States such as Germany.⁵⁶ Crucial here is less the quantity of inspections, but rather whether it takes place for a specific cause or regardless of any reason.⁵⁷ The ban of general monitoring obligations refers to inspections that are not triggered by a specific notification of the rightholder and which concern the complete content of the offer (of the platform). On the other hand, obligations that are imposed on the provider by a court or by authorities are not covered by the ban⁵⁸ and, by reason of a specific case, require, e.g., to eliminate a specific infringement. Thus, specific monitoring obligations subsequent to an order to prevent a similar breach of the law (“stay-down”) are not covered by the ban on non-prompted monitoring obligations⁵⁹ - which the CJEU

56 Higher Regional Court Hamburg MMR 2006, 744, 747; Altenhein, § 7 TMG para 6 in Joecks/Miebach (eds), *Münchener Kommentar zum StGB* (3 edn, CH Beck 2019); Hoffmann/Volkman § 7 TMG paras 33 ff. in Spindler/Schuster (eds), *Recht der elektronischen Medien* (4th edn, CH Beck 2019); *Holznapel/Höfing* (n 43), part 18.1 paras 54 ff.; Matthias Leistner, “Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet” [2012] ZUM 722, 724 with reference to the jurisdiction since Federal Court of Justice MMR 2007, 634, 637 with comments by Köster/Jürgens.

57 Settled case-law Federal Court of Justice MMR 2004, 668, 671 f. with comments by Hoeren; Federal Court of Justice MMR 2007, 507, 511 with comments by Spindler; Federal Court of Justice GRUR 2008, 702, 705; Federal Court of Justice, GRUR 2011, 152 para 48 I, on this matter: Gerald Spindler, *Präzisierungen der Störerhaftung im Internet* Besprechung des BGH-Urteils “Kinderhochstühle im Internet” [2011] GRUR 101; Federal Court of Justice GRUR 2011, 1038; Federal Court of Justice GRUR 2013, 370 with comments by Hühner; Federal Court of Justice, GRUR 2013, 1229 para 35; Federal Court of Justice GRUR 2015, 485 para 51; Federal Court of Justice GRUR 2015, 1129 para 37; Federal Court of Justice GRUR 2016, 855.

58 Recital (47) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (EC-Directive), OJ L 178/1/6; Government bill to § 8 (2) no 1 TDG, printed materials from the German Federal Parliament 14/6098, p. 23; Jandt, § 7 TMG para 44 in Roßnagel (ed), *Beck’scher Kommentar zum Recht der Telemediendienste*, (1st edn, CH Beck 2013); Paal (n 43) § 7 TMG para 52.

59 Federal Court of Justice MMR 2004, 668, 671 f. with comments by Hoeren; Federal Court of Justice GRUR 2011, 1038; Federal Court of Justice GRUR 2013, 370 with comments by Hühner; Federal Court of Justice, GRUR 2013, 1229 para 44; on the

55 CJEU Case C-360/10 SABAM v Netlog, EU:C:2012:85.

in the decision *Glawischnig-Piesczek* has recently confirmed.⁶⁰ However, Art. 15 (2) ECD allows (only!) national authorities to oblige providers to provide information about alleged unlawful activities or information.⁶¹ However, this exception does not apply to private law claims.

- 56 In the field of trademark law, the CJEU held the same view in the decision *L'Oréal versus eBay*⁶² regarding court orders against the service provider eBay concerning similar infringements:

“139 First, it follows from Art. 15 (1) of Directive 2000/31, in conjunction with Art. 2 (3) of Directive 2004/48, that the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider’s website. Furthermore, a general monitoring obligation would be incompatible with Art. 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly.

140 Second, as is also clear from Art. 3 of Directive 2004/48, the court issuing the injunction must ensure that the measures laid down do not create barriers to legitimate trade. That implies that, in a case such as that before the referring court, which concerns possible infringements of trade marks in the context of a service provided by the operator of an online marketplace, the injunction obtained against that operator cannot have as its object or effect a general and permanent prohibition on the selling, on that marketplace, of goods bearing those trade marks.”

- 57 Even if the CJEU does not explicitly enter into a fundamental rights assessment here,⁶³ these reasons do again show, that the service provider does not have to check the complete content initiatively for any possible violation.

scope of specific audit requirements Daniel Holznel, *Notice and Take-Down-Verfahren als Teil der Providerhaftung* (1st edn, Mohr Siebeck 2013) 109 ff.; Fabian v. Samson-Himmelstjerna, *Haftung von Internetauktionshäusern* (1st edn, CH Beck 2008) paras 356 ff.

60 CJEU Case C-18/18 *Glawischnig-Piesczek*, EU:C:2019:821; see on this matter Gerald Spindler, “Weltweite Löschungspflichten bei Persönlichkeitsrechtsverletzungen im Internet“ [2019] NJW 3274.

61 See also Recital (26) ECD.

62 CJEU Case C-324/09 *L'Oréal*, EU:C:2011:474.

63 To some extent in CJEU Case C-324/09 *L'Oréal*, EU:C:2011:474 para 143 with reference to the *Promusicae*-Decision of the CJEU.

Accordingly, orders against service providers that oblige them to identify the participants on the platforms are permissible (despite the required data protection), as well as to prevent similar infringements.⁶⁴

- 58 In addition, constitutional courts such as the European Court of Human Rights expressly referred to “chilling effects”⁶⁵ on the freedom of expression of the users due to a general control of the communication behavior, as well as due to “overblocking” of legally compliant contents.⁶⁶ With regard to the DSMD, the obligation to filter content and the shift of action to the user which have to claim their rights individually against the service provider is likely to lead to an inactivity of users, even if they are justified, and, on the other hand, to a blocking of content in case of doubt by service providers in order to avoid sanctions, thus resulting in “chilling effects” against freedom of expression.⁶⁷

b) Application to Art. 17 DSMD

- 59 It is questionable whether the constellation underlying the *Netlog* decision is comparable to Art. 17 DSMD – and as such would fall victim to the verdict of European illegality concerning fundamental rights. As already stated, this would not be the case for Art. 17 (4) (b) DSMD, since inspections by the service provider relates only to information provided by the rightholder; a general monitoring

64 CJEU Case C-324/09 *L'Oréal*, EU:C:2011:474 paras 142 ff.

65 Regarding “chilling effects” resp. references to the term in connection with freedom of expression, see for instance Federal Constitutional Court, NJW 2006, 207, 209; *Thoma v Luxembourg* App. no. 38432/97 (ECtHR 29 March 2001) para 58; *Standard Verlags GmbH v Austria* App. no. 13071/03 (ECtHR 2 November 2006) para 49; CJEU, joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, EU:C:2014:238, para 37; on the express use of the term “chilling effects” in connection with the *Netzwerkdurchsetzungsgesetz* (NetzDG) by the German Federal Government, see also the government bill on the NetzDG, p. 24; critical in this respect Nikolaus Guggenberger, “Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht” [2017] ZRP 98, 100.

66 See also the detailed case-law overview on the concept of “chilling effects” at <https://www.telemedicus.info/article/2765-Chilling-Effects-UEbersicht-ueber-die-Rechtsprechung.html> with further extensive references.

67 Similar Katharina Kaesling, “Die EU-Urheberrechtnovelle – der Untergang des Internets?” [2019] JZ 586, 589; Gielen/Tiessen (n 5) 639, 645, who is speaking of “overblocking” in this case; Maximilian Becker, “Von der Freiheit, rechtswidrig handeln zu können“ [2019] ZUM 636, 641.

or inspection of fundamental significance is not implied as this obligation depends explicitly upon information given by rightholders, hence, not regardless of such information and not proactively so that the principles of the Netlog decision would not intervene.⁶⁸

- 60 However, to consider only Art. 17 (4) (b) DSMD would - as indicated - fall too short:⁶⁹ Primarily, Art. 17 (1), (4) (a) DSMD forces the service provider to inspect all content in order to determine whether any content on his platform violates copyrights of rightholders - since as stated above, Art. 17 (1) DSMD extends the right of public availability onto the service provider, and therefore, makes him an immediate culprit. The service provider must therefore - as formulated in Art. 17 (4) (a) - “make every effort” to obtain licences. Only if he has failed to do so (Art. 17 (4) (a): “and”) Art. 17 (4) (b) DSMD intervenes. However, this compellingly requires that the service provider ensures himself regarding the existing contents and their legal situation;⁷⁰ otherwise the obligation in Art. 17 (1) (4) (a) DSMD to obtain licenses makes no sense. Which licenses should he obtain if the service provider does not know which content requires a license? Hence, as a first step the service provider has to check and to reassure himself which content has to be licensed. Hence, he has to proactively control the content - without regard to any information given by rightholders, and not restricted to such an information. Thus, the principles stated by the CJEU in the Netlog decision are clearly violated as Art. 17 (1), (4) a) DSMD introduces a proactive obligation to inspect without restrictions, such as in art. 17 (4) b) DSMD concerning information provided by rightholders.
- 61 This also applies to interpretation efforts by some authors that, given the complex rights collection and impossibility to control all content, are based on the principle of proportionality and only require the service provider to “moderate due diligence”.⁷¹ This may apply with regard to obtaining licenses itself, but does not change the fact that in the first instance all content has to be inspected to see if it violates any rights at all, and if so which. Since the obligation under Art. 17 (1), (4) (a) DSMD - and not under Art. 17 (4) (b) DSMD - resembles the general inspection claimed for in the Netlog case, such an obligation violates the ban on the general

monitoring obligation.⁷² In other words, Art. 17 (1), (4) (a) DSMD infringes the appropriate consideration of the affected fundamental rights, of the providers, as well as of the affected users, towards those of the rightholders.

- 62 In this context, as a precautionary measure, the term “upload filter” is inappropriate insofar as not just the controlling during the uploading of user-generated content is at stake, but the general monitoring of content on the platform - due to the obligation to obtain licenses.
- 63 It should also be considered that according to the system of Art. 17 (4) and (9) DSMD - the appeal procedure - content is first disabled or blocked and is only released after a complaint by the user. This creates, however, the above-mentioned “chilling effects” for freedom of expression, especially when content refers to current events⁷³ to which the complaint procedure would not be adequate due to loss of time. This is most evident when livestreams are blocked for which a complaint procedure results in the loss of the live character as they will be unlocked only after the streamed event.⁷⁴ Again, it would be more than unclear what “moderate due diligence” would mean, as the service provider would have to quasi constantly or at least randomly check the livestream in order to constantly monitor the legality of the streaming.
- 64 Finally, there is reason to fear that, even under Art. 17 (4) (b) DSMD, when restricting monitoring of the content supplied by rightholders, these lists of content will be so comprehensive that in fact a general monitoring of all content does occur.⁷⁵
- 65 Some authors plead for a restrictive interpretation of Art. 17 (4) DSMD in order to prevent the EU fundamental rights being violated due to the general monitoring duty.⁷⁶ Accordingly, the service providers should be supposed to act only upon pursuant information and notification and should obtain licences subsequently (!). This should be

68 Also Gielen/Tiessen (n 5) 639, 644; Peters/Schmidt (n 16) 1006, 1015.

69 Nevertheless for this view Peters/Schmidt (n 16) 1006, 1015.

70 To some extent Wandtke/Hauck, (n 22) 627, 635 f.

71 See Hofmann (n 12) 1224.

72 Similar doubts in Gielen/Tiessen (n 5) 639, 644; see also Martin Senftleben, “Filterverpflichtungen nach der Reform des europäischen Urheberrechts - Das Ende der freien Netzkultur?” [2019] ZUM 369, 372.

73 Senftleben (n 72) 369 372 f.

74 This was rightly pointed out by Henrik Weiden, “EU-Urheberrechtsnovelle auf der Zielgeraden?” [2019] GRUR 370, 372 and Gielen/Tiessen (n 5) 639, 645 hin.

75 Senftleben (n 72) 369, 372, who concludes that this is a violation of EU fundamental rights.

76 Affirmative Volkmann (n 12) 376, 378 paras 21 ff.

justified by Recital 66 (5) DSMD, as well as by Art. 17 (4) (b) DSMD.⁷⁷ However, this position fails to recognize the two-tier system of Art. 17 (1), (4) (a) and (4) (b) DSMD; the fact that the liability privilege of Art. 17 (4) (b) DSMD depends on the fact that the service provider has beforehand or in advance (!) made an effort to obtain licences etc. cannot be denied. Accordingly, Recital 66 (5) DSMD also does not refer to Art. 17 (1), (4) (a) DSMD, but to Art. 17 (4) (b) und c) DSMD,⁷⁸ which is clearly identifiable on the basis of the wording.

2. Counter-tendencies in the Case-Law of the CJEU and the Significance for Art. 17 DSMD

66 However, it must be borne in mind that the case law of the CJEU also shows opposing tendencies. As the CJEU in the UPC Telekabel decision⁷⁹ has basically recognized that access providers may be obliged to block websites; such blocking injunctions concern fundamental rights of users, providers and rightholders. Similarly, the CJEU delineated recently in the Glawischnig-Piesczek v. Facebook decision⁸⁰ general monitoring obligations from specific ones.

a) Disabling Obligations of the Access Provider

67 In the UPC Telekabel decision, the CJEU again stresses the statement, already made in Netlog and before that in the Promusicae decision, that a careful balance must be struck between the fundamental rights of rightholders on the one hand and that of users and providers on the other:

“46 The Court has already ruled that, where several fundamental rights are at issue, the Member States must, when transposing a directive, ensure that they rely on an interpretation of the directive which allows a fair balance to be struck between the applicable fundamental rights protected by the European Union legal order. Then, when implementing the measures transposing that directive, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with that directive but also ensure that they do not rely on an interpretation of it which would be in conflict with those

77 Expressly Volkmann (n 12) 376, 378 paras 24 ff., same direction Pravemann (n 22) 783, 787; Grisse (n 29) 897.

78 Correctly Pravemann (n 22) 783, 787, insofar contradictory.

79 CJEU Case C-314/12 *UPC Telekabel*, EU:C:2014:192.

80 CJEU Case C-18/18 *Glawischnig-Piesczek*, EU:C:2019:821.

fundamental rights or with the other general principles of EU law, such as the principle of proportionality (see, to that effect, Case C-275/06 Promusicae [2008] ECR I-271, paragraph 68).”

68 With regard to the right of entrepreneurial freedom, however, the CJEU considers that there is no restriction on the right in selection of agents for the providers and the subsequent discharge of liability:

“52 First, an injunction such as that at issue in the main proceedings leaves its addressee to determine the specific measures to be taken in order to achieve the result sought, with the result that he can choose to put in place measures which are best adapted to the resources and abilities available to him and which are compatible with the other obligations and challenges which he will encounter in the exercise of his activity.

53 Secondly, such an injunction allows its addressee to avoid liability by proving that he has taken all reasonable measures. That possibility of exoneration clearly has the effect that the addressee of the injunction will not be required to make unbearable sacrifices, which seems justified in particular in the light of the fact that he is not the author of the infringement of the fundamental right of intellectual property which has led to the adoption of the injunction.”

In view of the above-mentioned obligations according to Art. 17 (1) DSMD, this is certainly of importance as the liability-relieving effect is seemingly used by the CJEU in order to rule out a violation of fundamental rights.

69 However, the CJEU also emphasizes the protection of users' (basic) rights with regard to their freedom of information:

“56 In this respect, the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued.

57 It must be possible for national courts to check that that is the case. In the case of an injunction such as that at issue in the main proceedings, the Court notes that, if the internet service provider adopts measures which enable it to achieve the required prohibition, the national courts will not be able to carry out such a review at the stage of the enforcement proceedings if there is no challenge in that regard. Accordingly, in order to prevent the fundamental rights recognised by EU law from precluding the adoption of an injunction such as that at issue in the main proceedings, the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known.”

- 70 Again, for Art. 17 DSMD, it is important that users can assert their rights to a sufficient extent and with procedural certainty, let it be freedom of information or freedom of expression (and here e.g. freedom of citation etc., Art. 17 (7) et seq. DSMD).⁸¹
- 71 The obligation of access providers to block websites therefore affects the freedom of information under Art. 11 (1) sent. 2 ECFR,⁸² since disabling access to content constitutes a hindrance of informing the internet user. The freedom of information protects the simple use of information as well as the active procurement of the same,⁸³ in particular if access to information is definitively denied.⁸⁴ It cannot be excluded that - due to the usually not 100% error-free working filter systems - besides the blocking of impermissible content also permissible content might be disabled, hence resulting in a significant impairment regarding the freedom of information of users (so-called overblocking).⁸⁵ Exactly at this point parallels to uploading content filters of service provider servers are obvious.

81 More details below C.I.4.

82 See also the order for reference of the Federal Court of Justice GRUR 2016, 268; Anja Wilkat, *Bewertungsportale im Internet* (1st edn, Nomos 2013), 78 f.

83 Federal Constitutional Court NJW 1970, 235, 237; Helmuth Schulze-Fielitz, Art. 5 Abs. 1, 2 GG para 83 in *Dreier Grundgesetz Kommentar: GG* (3rd edn, CH Beck 2013); Christian Starck, Art. 5 Abs. 1, 2 GG para 40 in v. Mangoldt/Klein/Starck (eds), *Grundgesetz Kommentar* (7th edn, CH Beck 2018).

84 Federal Constitutional Court NJW 1970, 238, 240.

85 However, individual “false positive hits” should not lead to the inadmissibility of the measure, similar Matthias Leistner, “Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet“ [2012] ZUM 722, 732 f.; a too high number of “false positives” can also be prevented by manually checking the filter results, see Higher Federal Court Hamburg MMR 2016, 269 para 429 with comments by Frey; regarding overblocking CJEU Case C-314/12 *UPC Telekabel*, EU:C:2014:192, GRUR 2014, 468 para 56 with comments by Marly; CJEU Case C-484/14 *McFadden*, EU:C:2016:689, GRUR 2016 1146 para 93 f.; Federal Court of Justice GRUR 2016, 268; Georg Nolte and Jörg Wimmers, “Wer stört? Gedanken zur Haftung von Intermediären im Internet - von praktischer Konkordanz, richtigen Anreizen und offenen Fragen“ [2014] GRUR 16, 22; Gerald Spindler, “Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil “UPC Telekabel“ [2014] GRUR 826, 829, 834; Gerald Spindler, “Sperrverfügungen gegen Access-Provider - Klarheit aus Karlsruhe?“ [2016] GRUR 451, 455, 457; Matthias Leistner and Karina Grisse, “Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2)“ [2015] GRUR 105, 108 with further references.

b) Examination of Synonymous Content as Specific Monitoring Obligations

- 72 Even more clearly than in the decision of UPC Telekabel, the CJEU in the recent decision of *Glawischnig-Piesczek versus Facebook Ireland*⁸⁶ dealt with the delimitation of (prohibited) general monitoring obligations versus (permitted) specific monitoring obligations, as listed in recital 47 of the E-Commerce Directive, with regard to identical content (here: defamations etc.). In this context, the CJEU believes that a duty of the service provider to delete or block synonymous content would not lead to a general, especially not **active** monitoring obligation:

“37 In those circumstances, in order to ensure that the service provider at issue prevents any further impairment of the interests involved, it is legitimate for the court having jurisdiction to be able to require that service provider to block access to the information stored, the content of which is identical to the content previously declared to be illegal, or to remove that information, irrespective of who requested the storage of that information. In particular, in view of the identical content of the information concerned, the injunction granted for that purpose cannot be regarded as imposing on the service provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity, as provided for in Art. 15(1) of Directive 2000/31.”

- 73 However, the CJEU also recognizes that such an obligation on the part of the service provider may be accompanied by a substantive control of the “synonymous” content, which may in some circumstances lead to a general monitoring obligation when every single content uploaded by users has to be reviewed, in particular whether the relevant (new) content is largely similar or identical to the incriminated content. Therefore, the CJEU tries to limit these obligations:

“45 In light of the foregoing, it is important that the equivalent information referred to in paragraph 41 above contains specific elements which are properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal. Differences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the service provider concerned to carry out an independent assessment of that content.

46 In those circumstances, an obligation such as the one described in paragraphs 41 and 45 above, on the one hand - in so far as it also extends to information with equivalent

86 CJEU Case C-18/18 *Glawischnig-Piesczek*, EU:C:2019:821; see also Spindler (n 44) 3274.

content — appears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the service provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the service provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies.”

- 74 Accordingly, for the assumption of a specific monitoring obligation (which is permissible) it is sufficient that the provider can use automated techniques and that “specific details” are stated that allow a simple (probably automated) verification of similarity. In other words, the CJEU considers the use of automated technologies to be sufficient based upon “specific details” so that an active, general monitoring obligation by the provider is not yet assumed.
- 75 It is worth noting in this context that the CJEU does not carry out a fundamental rights assessment in contrast to the previous judgments, but instead sticks to abstract considerations with regard to the ban of general monitoring obligations in Art. 15 ECD. Nor is there any mention of opposing rights of the concerned users.

c) Application to Art. 17 DSMD

- 76 Applying the arguments of the described decisions of the CJEU to Art. 17 DSMD shows that Art. 17 (4) (b) DSMD should withstand the test of the Glawischnig-Piesczek decision, since, on one hand, the rightholders have to deliver the necessary information to providers (“specific details”); on the other hand, the usage of automated tools is open for providers.
- 77 However, this does not affect the obligation under Art. 17 (1) (4) (a) DSMD (the obligation to check content in order to obtain licenses) since the provider must first of all check the legality of the content itself and explicitly cannot rely on specific details provided by others that allow the usage of automated tools.

3. Result

- 78 To sum up, even though in recent restrictive rulings the CJEU restricted the ban on general monitoring duties, the Art. 17 (1) (4) (a) DSMD is prone to

violating fundamental constitutional rights of the ECFR as it introduces active investigation obligations of the provider, which are not compatible with the principles developed by the CJEU in SABAM / Netlog as well as in the L’Oréal decision.

- 79 Therefore, it can only be questionable whether a European constitution-compliant interpretation can suffice to establish the necessary balance of fundamental rights or to reconcile the duty of content control with the prohibition of general monitoring obligations. Thus, it is alleged that the effects of Art. 17 (8) DSMD or the prohibition of general monitoring obligations on Art. 17 (4) (a) DSMD must be taken into account when interpreting Art. 17 (1), (4) a) DSMD. The necessary “efforts” should therefore be interpreted accordingly.⁸⁷ Apart from the fact that it remains completely unclear how this should be managed; specifically how the required effort (according to which criteria?) should be construed, such an approach would ignore the clear wording and system of Art. 17 DSMD. The general content control contained in Art. 17 (1) DSMD is not limited by a reduction e.g., to evidently unlawful content (e.g., following the approach of Art. 14 ECD), since Art. 17 (1) DSMD does not contain such a restriction.

IV. Data Protection and Fundamental Rights

- 80 Furthermore, the intended obligations of the service provider in Art. 17 (1), (4) (a), (b) DSMD could also constitute an interference with the data protection principles under Art. 7 ECFR. Art. 17 no. 9 subsection 2 DSMD emphasizes:

“This Directive shall in no way affect legitimate uses, such as uses under exceptions or limitations provided for in Union law, and shall not lead to any identification of individual users nor to the processing of personal data, except in accordance with Directive 2002/58/EC and Regulation (EU) 2016/679.”

- 81 However, in order to prevent the uploading of unlawful content, the identity, specifically personal data (account holder etc.) could be checked. Up to now it is unclear if identity or other personal data can actually be separated from the content - which is a technical and factual question. Regarding blocking orders against access providers the CJEU assumed

87 Gert Würtenberger and Stephan Freischem, “Stellungnahme des GRUR Fachausschusses für Urheber- und Verlagsrecht (...)“ (GRUR-Statement) <http://www.grur.org/uploads/tx_gstatement/2019-09-05-GRUR-Stellungnahme_zur_DSM-_und_zur_Online_SatCab-RL_endg.pdf> accessed 26 November 2019, 57 ff.; similar Volkmann (n 12) 376, 382 paras 52 ff.

such an interference with data protection rights,⁸⁸ because the filtering or blocking measures of the access provider affected the IP addresses of the users, which may result in an impairment of the users' right of informational self-determination.⁸⁹ However, as mentioned above, the CJEU considered in the L'Oréal decision identification by service providers as permissible in order to prevent infringements. Therefore, it is decisive how the inspections under Art. 17 (4) (b) DSMD are designed, in particular whether content can be decoupled from the identity of users; in this case (and complete anonymization), there would be no interference with Art. 7 ECFR.

V. Alternatively: Possible Compensation for the Protection of Fundamental Rights

82 If the CJEU would not follow the arguments brought forward here, at least there would have to be safeguards in order to guarantee the fundamental rights of those concerned:⁹⁰

- Service providers - with regard to their entrepreneurial freedom - may not be required to constantly maintain manual inspections. As the CJEU has expressly stated in the cited decisions concerning acceptable controls, only an automated review is reasonable; otherwise, the business models of the service providers would be unfeasible. Only in the case of platforms clearly focused on unlawful infringements - in accordance with the case law of the German High Federal Court of Justice - in exceptional cases can a manual review be required.⁹¹ A corresponding implementation for the protection of fundamental rights is therefore necessary.

- With regard to the protection of users' interests, in particular their freedom of expression and access to information, the users must be provided with procedural mechanisms in order to flag relevant contents so that automated tools cannot be applied ("flagging"). As stated above, on several occasions the CJEU has emphasized the importance of such rights for users to safeguard their fundamental rights.⁹² This content, from the start, must be sorted out of an automated control and should be subject to a manual, human assessment. As far as can be seen, an automated control considering the balance of freedom of expression and information with other rights, for instance by recognizing parody, is currently not available. Again, this is an EU constitutionally required implementation.

- Moreover, in order to safeguard the freedom of opinion and access to information of the users, a subjective right to enforce the limitations vis-à-vis the service provider and the rightsholder must be provided for in view of the limitations for users in Art. 17 (7) DSMD. Currently, such claims exist only with regard to limitations to technical protection measures (so called Digital Rights Management System, Art. 6 (4) InfoSoc Directive). Although Art. 17 (7) DSMD does not mention such a right explicitly, it could be derived by the main target of Art. 17 (7) DSMD⁹³ and also by constitutional requirements, regardless of contractual rights and obligations.⁹⁴
- Furthermore, there should be protection of service providers and users against the abuse of rights by so-called "copyright trolls".⁹⁵ Otherwise, it cannot be excluded - in particular with regard to the US experience in the context of improper access notices (Digital Millennium Copyright Act) - that a reporting of alleged rights to service providers can be (mis-)used in order to delete or block certain content, e.g. in political campaigns.

88 Regarding Art. 8, 11 EU-CFR CJEU, Case C-70/10 *SABAM/Scarlet*, EU:C:2011:771 para; on this matter Gerald Spindler, "Anmerkung zu EuGH C-70/10" [2012] JZ 311 ff.; Markus Schröder, "Kommentar zu EuGH, Scarlet Extended" [2012] K&R 38; Stefan Maaßen, "Pflicht zur präventiven Filterung des gesamten Datenverkehrs zur Bekämpfung von Urheberrechtsverletzungen nicht mit europäischem Recht vereinbar - "Scarlet Extended" [2011] GRUR-Prax 535; Leistner (n 11) 722, 729.

89 Federal Court of Justice GRUR 2016, 268; agreeing Spindler (n 85) 451, 456.

90 For a more precise elaboration and scope for the Member States see below D.IV.5.

91 Federal Court of Justice ZUM 2013, 288 para 39.

92 See above C.III.2 for the UPC-Telekabel-Decision.

93 See below D.IV.2.

94 See above C.III.2 for the UPC-Telekabel-Decision.

95 See David Pachali, "Copyright Trills and presumptively fair uses" (iRights info, 09 July 2013 <<https://irights.info/webschau/der-urheberrechts-troll-und-mittel-gegen-ihn/15727>> accessed 15 November 2019); Brad A. Greenberg, "Copyright Trolls and Presumptively Fair Uses" (2014) University of Colorado Law Review Vol. 85, 53 ff.

D. Implementation of Art. 17 DSMD in National Law

I. Fully Harmonizing Character

83 Due to the fact that the purpose of the directive is to achieve a uniform level in the single market, Art. 17 DSMD is conceived as a fully harmonizing provision.⁹⁶ Consequently, neither Art. 17 DSMD contains any explicit opening clause for the Member States, nor are there any indications in the recitals to Art. 17 DSMD (Recitals 61 - 71) that the Member States would be permitted to tighten up the provisions or define certain aspects in a more distinguished way. In accordance with these provisions, the first known implementation draft at national level - the Dutch draft law - only provides for a more or less literal implementation.⁹⁷

84 Therefore, neither Art. 17 (1), (4) (a) nor (4) (b) DSMD can be “waived” by the Member States or specified on a larger scale – likewise, the Member States are not allowed not go beyond the provisions. However, Art. 17 (1), (4) a), b) DSMD do not prescribe specifically how or in which procedure the required efforts are to be determined at the national level. Whether there is still leeway for the Member States is discussed further below.

85 Furthermore, with regard to the provisions of Art. 17 (7) et seq. DSMD, the more recent case law of the CJEU must be considered. Considering the decisions in the Funke Medien Gruppe and Spiegel Online cases, the CJEU has clearly stated that the limitations provided for in the InfoSoc Directive are exhaustive and cannot be extended by national law⁹⁸ unless they themselves contain a leeway for the Member States to fill in vague legal terms.⁹⁹ Thus, the CJEU opens up a (moderate) scope for the Member States to specify the undefined legal concepts, which, however, must strictly adhere to the requirements of Union law, in particular the objectives of the DSMD.

86 The CJEU states in the Funke Medien Gruppe case that the necessary coherence must be maintained and:

“62 In that context, to allow, notwithstanding the express intention of the EU legislature, set out in paragraph 56 above, each Member State to derogate from an author’s exclusive rights, referred to in Articles 2 to 4 of Directive 2001/29, beyond the exceptions and limitations exhaustively set out in Article 5 of that directive, would endanger the effectiveness of the harmonisation of copyright and related rights effected by that directive, as well as the objective of legal certainty pursued by it (judgment of 13 February 2014, Svensson and Others, C466/12, EU:C:2014:76, paragraphs 34 and 35). It is expressly clear from recital 31 of the directive that the differences that existed in the exceptions and limitations to certain restricted acts had direct negative effects on the functioning of the internal market of copyright and related rights, since the list of the exceptions and limitations set out in Article 5 of Directive 2001/29 is aimed at ensuring such proper functioning of the internal market.”

87 Especially since Art. 17 (7) ff. DSMD does not contain any opening clause for Member States, Member States cannot go beyond the limitations provided for in Art. 17 (7, 9) DSMD.

88 However, the CJEU also stated in the cases of Spiegel Online and Funke Medien Gruppe¹⁰⁰, that:

“... the Member States are not in every case free to determine, in an un-harmonised manner, the parameters governing those exceptions or limitations”.¹⁰¹ In this context “the Member States are also required (...) to comply with the general principles of EU law, which include the principle of proportionality, from which it follows that measures which the Member States may adopt must be appropriate for attaining their objective and must not go beyond what is necessary to achieve it”¹⁰²

“... the discretion enjoyed by the Member States in implementing the exceptions and limitations provided for in Art. 5(2) and (3) of Directive 2001/29 cannot be used so as to compromise the objectives of that directive that consist, as is clear from recitals 1 and 9 thereof, in establishing a high level of protection for authors and in ensuring the proper functioning of the internal market”¹⁰³

96 Peters/Schmidt (n 16) 1006, 1011; Kaesling (n 67) 586, 590.

97 See below D.V.

98 CJEU Case C-469/17 *Funke Medien Gruppe* EU:C:2019:623 para 62; CJEU Case C-516/17 *Spiegel Online* EU:C:2019:625 paras 42 ff.

99 See CJEU Case C-516/17 *Spiegel Online* EU:C:2019:625 paras 25 ff.

100 Almost identical in wording CJEU Case C-469/17 *Funke Medien Gruppe* EU:C:2019:623 paras 43 ff.

101 CJEU Case C-516/17 *Spiegel Online* EU:C:2019:625 para 31 with reference to CJEU Case C-245/00 *SENA* EU:C:2003:68 para 34, CJEU Case C-145/10 *Painer* EU:C:2011:798 para 104, CJEU Case C-201/13 *Deckmyn and Vrijheidsfonds* EU:C:2014:2132 para 16.

102 CJEU Case C-516/17 *Spiegel Online* EU:C:2019:625 para 34.

103 CJEU Case C-516/17 *Spiegel Online* EU:C:2019:625 para 35.

“... the three-step test practiced under Art. 5 (5) InfoSoc-Directive has to be complied with”¹⁰⁴

“... the principles enshrined in the Charter apply to the Member States when implementing EU law. It is therefore for the Member States, in transposing the exceptions and limitations referred to Art. 5 (2) and (3) of Directive 2001/29, to ensure that they rely on an interpretation of the directive which allows a fair balance to be struck between the various fundamental rights protected by the European Union legal order”.¹⁰⁵

- 89 In conclusion, there is always the risk that the CJEU will narrow the scope for the implementation opened up by vague legal terms.¹⁰⁶ Therefore, and especially with regards to the EU-Commission’s competence to issue guidelines under Art. 17 (10) DSMD, it is recommended to work with provisions that provide for deviation in an individual case.¹⁰⁷

II. Implementation of the Definitions of Art. 2 (6) DSMD

- 90 With regard to the various definitions for the service providers affected under Art. 2 (6) DSMD, the national legislator can quantitatively fill in and specify the “large” number of content - but with the risk that in individual cases the CJEU will consider the number chosen to be unrepresentative. Furthermore, the purpose of the definition, namely the role of service providers, particularly the element according to which the platform acts as a substitute for traditional forms of distribution, should be included in the implementation of the definition, as well as, conversely the exception for platforms which promote piracy.
- 91 Other specifications, e.g., of the feature “organised”, are not advisable; in contrast, implementing provisions that work with principle examples would be preferable, e.g. the ability to find content with search tools, as they allow for deviations in specific cases whilst providing more legal certainty.
- 92 The negative definition should accordingly be codified literally by the national legislator, since in individual cases demarcation questions may arise which can hardly be determined in an abstract manner separately from the concrete facts.

104 CJEU Case C-516/17 *Spiegel Online* EU:C:2019:625 para 37.

105 CJEU Case C-516/17 *Spiegel Online* EU:C:2019:625 para 38.

106 Similar *Würtenberger/Freischem* (n 87) 50 ff.

107 *Würtenberger/Freischem* (n 87) 51 ff.

III. Restriction and Structuring of the Obligations of the Service provider

1. Obligations to Obtain Licenses According to Art. 17 (1), (4) (a) DSMD

- 93 As a consequence of the extension of the right to make available to the public Art. 17 (1) subpara. 2 DSMD provides in subparagraph 1 that:

“An online content-sharing service provider shall therefore obtain an authorisation from the rightholders referred to in Art. 3(1) and (2) of Directive 2001/29/EC, for instance by concluding a licensing agreement, in order to communicate to the public or make available to the public works or other subject matter.”

In addition, in the event that the license is not granted, Art. 17 (4) (a) DSMD requires with regard to exemption from liability:

“that they [service providers] have:

a) made best efforts to obtain an authorisation;”

- 94 As already mentioned, this results in the service provider’s obligations to review the content on its platform if licenses are required and to “make every effort” to obtain the permission. Art. 17 (1), (4) (a) DSMD do not provide for any opening clauses so that these requirements have to be implemented into national law. Concerning the principle of proportionality in Art. 17 (5) DSMD some authors argue that Member States have the power to “spell out” the implications of the flexibility of the DSMD – which should mean the exclusion of smaller or young entrepreneurs from the obligation to upload filters.¹⁰⁸ As already mentioned, however, such a general exclusion would contradict the explicit exception in Art. 17 (6) DSMD, which was politically highly controversial during the policy-making process.
- 95 Whether Art. 17 DSMD allows Member States to modify or substantiate the required high industrial standards is unclear. As Art. 17 (4) (a) (b) DSMD does not rely on a specific duty of supervision defined by the Member State rather than generally on the necessary efforts according to standards outside the law (industrial standards), these efforts cannot be restricted for instance to the search for “digital fingerprints” of copyrighted works (and leaving other content uninspected).
- 96 Furthermore, a duty for rightholders to register their rights in a state-monitored platform would

108 *Gielen/Tiessen* (n 5) 639, 643.

not be compatible with Art. 17 (1) DSMD since it does not stipulate how the service provider obtains information regarding necessary licenses; channeling to a platform for rightholders, where the service provider would solely need to access (one-stop-shop) would be desirable, but would come close to copyright registration which is not intended by TRIPS, WIPO, etc.¹⁰⁹

97 A national implementation which would restrict the efforts to a query of licenses from collecting societies is also confronted with the problem that even collecting societies do not always have the complete repertoire that would be necessary to license all kinds of content on the platform.¹¹⁰ Moreover, even though the application of Art. 12 DSMD (collective licensing) can partially remedy this situation, it does not relieve the service provider from checking all license offers. Similar problems exist with respect to the exploitation rights of non-professional authors such as amateur photographers or video producers, or text authors - but Art. 12 DSMD can help here as well. This solution fails, however, when pan-European licenses are required, which also do not exist in all cases - it is not even possible to regulate this aspect through Art. 12 DSMD (“on their territory”).¹¹¹ To define the obligations of the service provider therefore on a national level in such a way that a query by a collecting society alone would in the end be sufficient, is not properly implementing Art. 17 (1) (4) (a) DSMD.

98 It is therefore conceivable, but also recommendable, that the Member State outlines the requested efforts by using a sample catalogue (catch-up clause), which, however, should by no means be exhaustive. This can be codified by an “in particular” clause listing individual services by volume, revenue, number of users, content, etc., for which a catalogue of graduated efforts can then apply. For example, a presumption can be established for the fulfillment of the requested effort that queries to collecting societies can be sufficient for the necessary efforts;¹¹² even more so when these offer collective licenses according to Art. 12 DSMD yet leaving it to the specific case if more efforts are necessary. The same could apply with regard to very small content or personal content which are difficult to determine in terms of authorship, as well as the legal situation

(consent? intervening limitations?). Here it could be sufficient to oblige the service provider to conduct a single search. Such a presumption rule although should not be exhaustive.

99 However, it would not be sufficient to offer rightholders a “monetisation”¹¹³ – without any effort of service providers to obtain rights from them. This would amount to a reversal of the mechanism intended in Art. 17 (1) (4) (a) DSMD as rightholders would then have to seek licensing themselves.

100 A further specification of the efforts could be made by an implementing regulation on a national level, e.g., the number of searches for licenses or rights depending on the size of the platform. This could also be done by creating a governmental platform where rightholders can register their rights in a machine-readable form, which can then be retrieved (automatically) by the service provider. As long as such a specification of efforts would not end up in an exhaustive catalogue rather than in a presumption rule (leaving leeway for specific cases) Art. 17 DSMD does not withstand such a solution. Nor would such a presumption lead to the reversal of the burden of proof at the expense of the providers (“unless”) provided for in Art. 17 (4) DSMD. This reversal of the burden of proof relates to compliance with the standards to be demonstrated by the provider in individual cases; the here advocated presumption of conformity refers in contrast to the ascertainment of the standards themselves, which is not the same.

101 Finally, a clarification by the implementing legislator that it is permissible for the service provider to make the content available for the duration of license negotiations and the obtaining of “permits” seems to make sense.¹¹⁴ This results not least from the fact that the service provider still makes every effort to obtain licenses (Art. 17 (4) (a) DSMD) and therefore is not liable until these efforts are unsuccessful.

102 All in all, therefore, the possibilities of finally substantiating the efforts under Art. 17 (1) (4) (a) DSMD are limited and fraught with the risk of European illegality.

¹⁰⁹ Art. 9 (1) TRIPS-agreement in conjunction with Art. 9 Berne Convention.

¹¹⁰ See Henrike Weiden, “Aktuelle Berichte – April 2019“ [2019] GRUR 370, 371.

¹¹¹ See for the problems concerning licensing Senftleben (n 72) 369, 371.

¹¹² See also Gielen/Tiessen (n 5) 639, 643.

¹¹³ See Hofmann (n 12)1225; Würtenberger/Freischem (n 87) pp. 50 ff.

¹¹⁴ This is rightly pointed out by Dreier (n 28) 776.

2. Limitation and design of upload filters according to Art. 17 (4) (b) DSMD

a) Exclusion of Upload Filters?

103 As explained above, Art. 17 (4) (b) DSMD is also fully harmonizing. Which procedures the service provider should apply is not further specified by Art. 17 (4) (b) DSMD; conversely, the freedom of the service provider to choose adequate tools within the limits of Art. 17 (4) (b) DSMD is not restricted. In any case, the procedures must meet “high industry standards”. Art. 17 (4) (b) DSMD thus refers to a non-legislative flexible standard which cannot be excluded or replaced by the national legislator.¹¹⁵ This is valid as well for automated tools (upload filters); as mentioned already, Art. 17 (9) subpara. 1 DSMD expressly mentions human handling of complaints, which makes clear that in other cases the procedures in Art. 17 (4) (b) DSMD can be automated - and consequently cannot be excluded by the implementing Member State.¹¹⁶

104 Some authors derive from the principle of proportionality in Art. 17 (5) DSMD that smaller or financially weak online platforms are exempt from the obligation to provide upload filters, since otherwise they would face insurmountable difficulties and new barriers to market entry would be erected which would also be in contradiction with the DSMD’s focus on innovation in the digital internal market. Therefore, Member States should have the power to “clarify” that such companies are only subject to the notice-and-take-down or stay-down obligation.¹¹⁷ However, as already argued, this view is diametrically opposed by the exception afforded to start-ups in Art. 17 (6) DSMD, which was the subject of numerous discussions in the trilogue procedure. The originally envisaged exceptions for small and medium-sized enterprises were thus much more extensive than in the final version of Art. 17 (6) DSMD.¹¹⁸ Only for the companies of Art.

17 (6) DSMD obligations of the service providers are reduced to Art. 17 (4) c) DSMD (notice-and-stay-down). This fundamental decision cannot be undermined via the “back door” of proportionality.¹¹⁹ A corresponding Member State exemption which would go beyond Art. 17 (6) DSMD and would be decoupled from the individual case (which otherwise has to be determined by courts in the context of the proportionality test), cannot be reconciled with Art. 17 (6) DSMD.

105 Finally, when some authors argue that the service provider in general (!) only has to act on the basis of a notification or information provided¹²⁰ this is only true with regard to the system of Art. 17 (4) (b) DSMD but not with regard to Art. 17 (1), (4) (a) DSMD); it does not change the fact it is necessary to install a filter for the information about these rights.¹²¹

b) Implementation

106 As explained above, Art. 17 (4) b) DSMD refers to high industry standards. However, the DSMD does not specify how these standards are to be defined, so that there is leeway for the Member States to define the procedures by which these standards are to be determined within the framework of the high standards customary in the sector. Within the framework of the implementation of Art. 17 (4) (b) DSMD, for example, committees and procedures could be set up here which may be comparable to national technical standardization - while at the same time ensuring that the state does not have any influence on the selection procedures or filters relevant for opinion-forming. At the same time, however, it must also be taken into account that these standards are “customary in the industry”, so that they must differentiate according to the type of service provider (e.g. video platforms such as YouTube and social networks such as Facebook).

107 How such standards are to be designed in concrete terms must be determined in cooperation with computer scientists and cannot be clarified within the framework of a legal opinion. The most

¹¹⁵ E.g. Kaesling (n 67) 586, 590; Senftleben (n 72) 369, 371; Hofmann (n 12) 1221.

¹¹⁶ Similarly Kaesling (n 67) 586, 590; Gielen/Tiessen (n 5) 639, 644; Volkmann (n 12) 376, 380 para 32.

¹¹⁷ Gielen/Tiessen (n 5) 639, 643 ff.; similar Hofmann (n 12) 1227.

¹¹⁸ See Axel Voss, Committee on Legal Affairs, Report on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market (COM(2016)0593 – C8-0383/2016 – 2016/0280(COD)), 29.6.2018, A-8-0245/2018, accessible at: http://www.europarl.europa.eu/doceo/document/A-8-2018-0245_EN.pdf

¹¹⁹ For a different opinion see Gielen/Tiessen (n 5) 639, 644, who state without any further justification that the exceptions in the DSMD “cannot be interpreted as a negative statement that all other online platforms must be covered by the obligation to filter. What the authors did not point out is why the considerable discussions regarding the start-up exemptions actually came up.

¹²⁰ See Volkmann (n 12) 376, 379 para. 29, who, however, only refers to a flat-rate filter obligation.

¹²¹ Similar Volkmann (n 12) 376, 379 para. 32 ff.

conceivable effective measure here would be the “flagging” of content by users, so that this content is automatically sorted out and subjected to human examination.

- 108** It would also be conceivable to regard certain users who have not committed any infringements in the past as “trusted uploaders” who would be excluded from a filter beforehand. According to Art. 17 (5) DSMD it would also be necessary to consider the extent or scope of a copyrighted work used in a content in relation to the entire content, which could be an indication of a quotation, even if - as will be explained further - the DSMD does not know any *de minimis* limit.
- 109** Finally, it would still be possible to exclude ambiguous content from an upload filter beforehand and to transfer them to a human check; such an exception could be supported by Art. 17 (5) DSMD within the context of proportionality which also takes the nature of the contents into account. This would include, for example, the CJEU’s orientation described above towards automated procedures for content with similar meaning. However, this would still leave open the question of when there are inconclusive infringements.
- 110** However, all these proposals are ultimately subject to the premise that a) the standards are customary in the industry and b) the standards are high. Accordingly, it is difficult to assess whether the Member State can determine that only those standards that have been established in the state-regulated procedure represent the due diligence that is customary in the industry. It is also unclear whether the Member State can finally regulate the standards in accordance with the above-mentioned proposals. Finally, the legal implication of complying with these standards remains unclear: does compliance with a standard mean complete exemption from liability or only a *prima-facie* proof that the necessary efforts have been met? As art. 17 (4) b) DSMD refers to those standards specifying the necessary efforts, Art. 17 (4) should indeed be read as a liability privilege – and not only some sort of evidence rule.
- 111** However, the implementing legislator could establish a presumption of conformity with the diligence required by Art. 17 (4) (b) DSMD if the standards adopted by state-regulated procedures are complied with. A violation of the burden of proof rule in Art. 17 (4) b) DSMD would not be associated with this, since only the evidentiary effect of the standard established by state-regulated procedures would be determined; the service provider would still have to explain and prove how it complied with this standard. If necessary, this procedure can also be combined with certifications which then initiate

the presumption of conformity.

- 112** If technically no filter is known in the industry, it remains the case that the service provider cannot be obligated to do something that is technically impossible.¹²² For example, the filter technology ContentID¹²³ is known from YouTube.¹²⁴ For social networks other criteria may then apply, e.g. the filters used by Facebook - which, however, are also subject to corresponding criticism.¹²⁵ Whether there are comparable technologies for other works, in particular movies, is doubtful at present.¹²⁶ This is especially the case regarding parodies etc., as shown by the well-known example of the RTL movie “Not Heidis Girl” whose parody character was not recognized by the filter used by Google.¹²⁷ Since Art. 17 (4) (b) DSMD refers to the standards customary in the industry, the obligations must be omitted if they simply do not exist in an industry.

122 Gielen/Tiessen (n 5) 639, 644 f.; Gerhard Pfennig, “Forderungen der deutschen Urheber und ausübenden Künstler zum Reformprozess des Urheberrechts der EU” [2018] ZUM 252, 255; Stieper (n 10) 211, 216.

123 How Content ID works see “Help Center: How Content ID works” <<https://support.google.com/youtube/answer/2797370?hl=de>> accessed 28 November 2019; Helmut Henrich, “Plattformen werden Verantwortung übernehmen” (*medienpolitik.net*, 16 April 2019) <<https://www.medienpolitik.net/2019/04/plattformen-werden-verantwortung-uebernehmen/>> accessed 17 April 2019.

124 See for the different filter technologies e.g. Kaesling (n 67) 588; Graziana Kastl, “Filter – Fluch oder Segen?” [2016] GRUR 671, 671 ff. with further proof.

125 See for corresponding deleting clauses, Gerald Spindler, “Löschung und Sperrung von Inhalten aufgrund von Teilnahmebedingungen sozialer Netzwerke” [2019] CR 238 ff. with further references.

126 A further development of Microsoft’s PhotoDNA, for example, an Upload filter, which is already said to be able to detect and block so-called revenge pornography and child pornographic material by using machine learning, would be conceivable here; however, technical details of the filter are not known yet; see Stefan Krempel, “Upload-Filter: Facebook und Instagram löschen Rache pornos automatisch” (*heise online*, 16 March 2019) <<https://www.heise.de/newsticker/meldung/Upload-Filter-Facebook-und-Instagram-loeschen-Rache-pornos-automatisch-4338270.html>> accessed 28 November 2019.

127 See Ingo Dachwitz and Alexandra Fanta, “Not Heidis Girls: Wie Youtube eine Kampagne gegen Sexismus ausbremste” (*Netzpolitik.org*, 6 March 2018) <<https://netzpolitik.org/2018/not-heidis-girl-wie-youtube-eine-kampagne-gegen-sexismus-ausbremste/>> accessed 28 November 2019.

113 Another general conflict between Member States' specifications and the DSMD could result out of Art. 17 (10) DSMD, which gives the EU Commission competence to define guidance for Art. 17 (4) DSMD according to a complex procedure with the participation of stakeholders. Recital 71 formulates the intended stakeholder dialogue in a similar way. Member States are mentioned only with regard to cooperation with the Commission. National stakeholder dialogues or standardization procedures are not mentioned in Art. 17 (10) DSMD. The guidelines to be issued by the Commission refer in their entirety to the procedures under Art. 17 (4) DSMD, and thus also to (4) b) and the high industry standards mentioned therein.

114 However, Art. 17 (10) DSMD is not completely clear, since Art. 17 (10) DSMD expressly speaks of "in particular regarding the cooperation referred to in paragraph 4", which probably means the information to be provided by the rightholders. On the other hand, Art. 17 (10) DSMD shows that the procedures under Art. 17 (4) (b) DSMD must also be meant, since otherwise the obligation of service providers or service providers to provide user organizations with access to appropriate information "on the functioning of their practices with regard to paragraph 4" makes hardly any sense.

115 As a result, the EU Commission has quasi "sovereignty" over the specification of the procedures under Art. 17 (4) b) DSMD - so that a Member State standardization procedure for Art. 17 (4) DSMD must respect the guidelines under Art. 17 (10) DSMD. However, under Art. 17 (10) DSMD, the Commission's guidelines do not have any legally binding effect towards courts or authorities; unlike authorizations for implementing Directives or Regulations, they are not legal acts with binding effect. Thus, the CJEU has determined in the context of antitrust proceedings that:

*"209 The Court has already held, in a judgment concerning internal measures adopted by the administration, that although those measures may not be regarded as rules of law which the administration is always bound to observe, they nevertheless form rules of practice from which the administration may not depart in an individual case without giving reasons that are compatible with the principle of equal treatment. Such measures therefore constitute a general act and the officials and other staff concerned may invoke their illegality in support of an action against the individual measures taken on the basis of the measures (see Case C-171/00 P Liberis v Commission [2002] ECR I-451, paragraph 35)."*¹²⁸

116 Rather, there is a certain degree of self-commitment

128 CJEU Joined Cases C189/02 P, C202/02 P, C205/02 P bis C208/02 P and C213/02 P *Dansk Rørindustri*, EU:C2005:408, para 209.

of the Commission;¹²⁹ (national) courts and authorities of the Member States must take into account the recommendations or guidelines, but may deviate from them.¹³⁰ It is therefore possible for the Member State to design the procedures for the high standards customary in the sector, but with the restriction that these must comply with the Commission's guidelines pursuant to Art. 17 (10) DSMD.

117 Beyond legal implementation Member States can support the development of upload filters at the political level by state funding or supporting committees and platforms (while at the same time maintaining distance from the state influence) which attempt to code automated processes by means of open source coding - and make them available to the general public for further development, in particular for small and medium enterprises.¹³¹

c) Information to be provided by rightholders

118 As explained above, the service provider is obliged under Art. 17 (4) b) DSMD (in contrast to Art. 17 (1), (4) a) DSMD) to monitor the content generated and uploaded by users only on the basis of the information on content provided by the rightholder. However, the DSMD does not specify how this information has to be provided. Thus, Member States may opt for certain specifications, e.g. with regard to machine readability of the information in order to facilitate the processing of the information. Such a specification, however, depends on whether the DSMD should be regarded exclusive in the sense that it is left to the rightholders to decide how they specifically provide information to the service providers and Member States cannot specify the ways and means of how to provide such information.

119 Such "negative" harmonization (with no leeway for Member States) would be supported by the fact that in

129 CJEU Joined Cases C189/02 P, C202/02 P, C205/02 P bis C208/02 P and C213/02 P *Dansk Rørindustri*, EU:C2005:408 para 211.

130 For an elaborated discussion on this topic, see Jürgen Schwarze, "Soft Law im Recht der Europäischen Union" [2011] EuR 3, 8 ff. with further references.

131 See the statement of the German government from 15 April 2019: Draft Directive of the European Parliament and of the Council on copyright and related rights in the Digital Single Market and amending Directives 96/6/EC and 2001/29/EC – Statements [2019] 2016/0280(COD), 7986/19 ADD 1 REV 2.

contrast to the DSMD other directives or regulations - such as Art. 20 (1) GDPR¹³² - expressly stipulate machine readability, for example with regard to data portability. The stakeholder dialogue in Art. 17 (10) DSMD also indicates that the national legislator has no discretion here. However, the national legislator could again work with presumption effects in favor of the service providers for certain procedures, e.g. platforms on which rightholders can register their content, but which are not conclusive and which take into account the EU Commission's guideline competence under Art. 17 (10) DSMD.

120 In this context, due to the danger of “copyright trolls” or unlawful rights information and thus potential blockades of (unwelcome) content, consideration should also be given to procedural requirements for the necessary identification of rightholders and the unambiguous, verifiable indication of rights, e.g. by so-called “trusted flaggers”, which must also apply to corresponding requests for deletion.¹³³ However, such a specification must also consider the guidance competence of the Commission according to Art. 17 (10) DSMD.¹³⁴

121 Not affected by Art. 17 (10) DSMD, however, is the introduction of rights of the involved users, including the introduction of a stricter liability for “copyright trolls” due to abusive notification of alleged rights. The national legislator has a great degree of flexibility here.¹³⁵ National case-law recognizes liability for unjustified warnings of industrial property rights, but these are linked to the right of the business established and practiced. On the other hand, the requirement of so-called “trusted flags” for trustworthy communications from rightholders within the framework of Art. 17 (4) b) DSMD would again be confronted with the

objection of infringement of Art. 17 (10) DSMD, which leaves it to the Commission to determine the form of such procedures; nevertheless, presumption rules with respect to Art. 17 (10) DSMD are possible.

3. Collective Licenses

122 Ultimately, the procedure of “extended collective licences” (also referred to as ECL), which is based on the Scandinavian model in accordance with Art. 12 DSMD, should be used, according to which rights (or rightholders) not represented by the collecting societies may also be licensed by them. This would allow service providers to obtain the necessary permissions while avoiding extensive searches to obtain rights.¹³⁶ However, this solution should not be overestimated, especially in terms of avoiding upload filters.¹³⁷ Licensing under Art. 12 DSMD depends on the rightholders not opting out of collective licensing, Art. 12 (3) (c) DSMD.¹³⁸ In particular, larger rightholders will make use of the opt-out possibility and exclude their rights from exploitation by collecting societies, as experience in the music and film markets¹³⁹ has already shown. In addition, licensing under Art. 12 (1) DSMD only concerns use in the territory of the respective Member State. If Art. 12 DSMD is not implemented in all Member States and reciprocity agreements between collecting societies are not concluded, then there will not be much effects of ECLs in order to avoid problems of licensing under the DSMD.¹⁴⁰

123 An implementation that would introduce mandatory collective licenses¹⁴¹ would contradict the CJEU's decision in the Soulier case¹⁴² in which the CJEU clearly emphasized the author's individual right to consent and prior information - and would not be covered by Art. 12 DSMD.

¹³² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); OJ L 119, p. 1–88 ss. of 4.5.2016; Art. 20 GDPR prescribes transmission for data portability “in a structured, commonly used and machine-readable Format”.

¹³³ Statement by the Federal Government at the vote in the Council of Ministers of 15 April 2019, Statements [2019] 2016/0280(COD), 7986/19 ADD 1 REV 2, point 8.

¹³⁴ Left open in Hofmann (n 12) 1228 who, however, is arguing that regulations under Art. 17 (10) of the DSMD have precedence.

¹³⁵ Württenberger/Freischem (n 87) p. 60.

¹³⁶ Agreeing Dreier (n 28) 771, 777 f.; Kaesling (n 67) 586, 589 f.; Gielen/Tiessen (n 5) 639, 643.

¹³⁷ Similar Martin Husovec and João Quintais, “How to Licence Art. 17?” (SSRN, 14 October 2019, p. 19) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463011> accessed 28 November 2019.

¹³⁸ Skeptical Hofmann (n 12) 1224.

¹³⁹ See especially Christine Wirtz, “Perspektiven des Urheberrechts im Informationszeitalter” [2019] ZUM 203, 206.

¹⁴⁰ This is rightly pointed out by Dreier (n 28) 771, 777 f.

¹⁴¹ Discussed by Husovec/Quintais (n 139) p. 22.

¹⁴² CJEU Case C-301/15 Soulier EU:C:2016:878.

IV. Regulatory limitations in favor of users

1. No additional statutory limitations in Member States

124 As mentioned above, the CJEU has recently ruled in several cases that the statutory limitations of the InfoSoc Directive, and thus also the DSMD, are exhaustive for Member States; they cannot go beyond that. Only within the framework of vague legal notions and in compliance with the above-mentioned criteria of the CJEU, the Member State can enjoy leeway for implementation.

125 For Art. 17 DSMD, this means that Member States cannot introduce a general statutory limitation for user-generated content, since neither Art. 17 (4) – (10) DSMD nor Art. 5 (2), (3) InfoSoc Directive provide for such a limitation for the right of communication to the public¹⁴³ (even if we consider the limitation of Art. 5 (2) b) InfoSoc Directive as the right to reproduction for private purposes to be relevant here, since this does not include the right of communication to the public). This applies all the more to service providers.

126 An attempt has been made on several occasions to justify a limitation to user-generated content by means of an extensive interpretation of the citation limitation and the limitation to pastiche, in particular in the light of freedom of expression pursuant to Art. 11 ECHR.¹⁴⁴ Others speak of “statutory licences” with an obligation to pay, which produce exactly the same effects as limitations, but are apparently supposed to be licenses.¹⁴⁵

127 However, in the light of the more recent decisions of the CJEU, in which the Court sets narrow limits for the Member States on the design of statutory limitations and denies new limitations on the national level, such an extension hardly seems possible. Particularly with regard to the right of quotation, remixes as arrangements do not fulfil the requirement of the pure use of a work to support one’s own ideas or the work.¹⁴⁶ A way to create some freedom for user-generated content would refer to the limitation for

pastiches (that has to be implemented in Member States), since pastiches are defined as “...a work of visual art, literature, theatre, or music that imitates the style or character of the work of one or more other artists”.¹⁴⁷ However, the national legislator will not be able to go beyond these concepts transposing the DSMD. It will therefore be left to the courts to define the limits and possibilities for user-generated content within the pastiche limitation.¹⁴⁸ The same applies to the attempt to establish “statutory licences”. As explained above, despite the different term these correspond to limitations and cannot hide the fact that compulsory licenses are subject to the same conditions. A different use of language alone will not change that.

128 Neither do Art. 17 DSMD nor the InfoSoc Directive contain any *de minimis* limit.¹⁴⁹ Accordingly, also for small-scale uses or uses without any economic value there is no separate limitation in favor of them.¹⁵⁰

129 However, a starting point for a different interpretation, in particular that the catalogue of limitations in Art. 17 (7) (2) DSMD is not exhaustive, would be the general (in fact self-evident) statement in Art. 17 (7) (1) DSMD that the cooperation between the service providers and the rights holders must not have the effect that content uploaded by users does not infringe copyrights or is “covered by an exception or limitation”. This would, however, also cover all the limitations under Art. 5 (2), (3) InfoSoc Directive - beyond those mentioned in the second subparagraph of Art. 17 (7) DSMD, since even if the limitations under Art. 5 (2), (3) InfoSoc Directive were to intervene, there would be no copyright infringement. In this way, the application of limitations in favor of science and research and education could also be justified within the framework of Art. 17 (7) DSMD, since these also cover the right of communication to the public within the framework of Art. 5 (3) a) InfoSoc Directive. However, the legislator must then also introduce a right for users to appeal against these limitations - which in turn conflicts with the exhaustive enumeration in Art. 17 (7), (9) DSMD.

¹⁴³ Following the stated opinion Hofmann (n 12)1221.

¹⁴⁴ See especially Senftleben (n 72) 369, 373.

¹⁴⁵ E.g. Husovec/Quintais (n 139) 23 f.

¹⁴⁶ Senftleben (n 72) 369, 373 comes to the same conclusion and calls for a new limitation for user-generated content beyond the right of quotation – which, however, according to the CJEU jurisprudence, will hardly be possible anymore.

¹⁴⁷ See “Pastiche” (*Wikipedia*, 19 November 2019) <<https://en.wikipedia.org/wiki/Pastiche>> accessed 29 November 2019.

¹⁴⁸ Similar Würtenberger/Freischem (n 87) 67.

¹⁴⁹ CJEU Case C-476/17 *Phonogram producer* EU:C:2019:624; For the DSMD Hofmann (n 12)1221; see already Spindler (n 24) 277, 290; for a different opinion contra legem see Torsten J. Gerpott, “Artikel 17 der neuen Eu-Urheberrechtsrichtlinie- Fluch oder Segen?” [2019] MMR 420, 424.

¹⁵⁰ See Würtenberger/Freischem (n 87) 67 f.

2. Right to enforce limitations against providers

130 Conversely, the national legislator is now obliged to introduce a subjective right for users to enforce the limitations based on the wording of Art. 17 (7) DSMD. This is clearly shown by the wording of Art. 17 (7) (2) DSMD:

“Member States shall ensure that users in each Member State are able to rely on any of the following existing exceptions or limitations when uploading and making available content generated by users on online content-sharing services:

(a) quotation, criticism, review;

(b) use for the purpose of caricature, parody or pastiche.”

131 If all users should be able to rely upon the exceptions, they must be granted a subjective right to enforce the exceptions, which in this form does not yet exist in some jurisdictions such as Germany, except within the framework of Art. 6 (4) InfoSoc Directive (here, however, against the rightholders!). This legal protection is even more clearly stated in Art. 17 (9) (2) DSMD:

“Where rightholders request to have access to their specific works or other subject matter disabled or to have those works or other subject matter removed, they shall duly justify the reasons for their requests. Complaints submitted under the mechanism provided for in the first subparagraph shall be processed without undue delay, and decisions to disable access to or remove uploaded content shall be subject to human review. Member States shall also ensure that out-of-court redress mechanisms are available for the settlement of disputes. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies. In particular, Member States shall ensure that users have access to a court or another relevant judicial authority to assert the use of an exception or limitation to copyright and related rights.”

Specifically, this explicit requirement that users should be able to enforce their rights before a court implies the introduction of binding subjective rights for users; otherwise users will not be able to file claims at courts.¹⁵¹

132 So far, German courts have assumed an independent contractual claim in case of social networks, partly based on a contract “sui generis”,¹⁵² especially in

¹⁵¹ Following the stated opinion Hofmann (n 12)1227.

¹⁵² Higher Regional Court Munich MMR 2018, 753, 754 para 18, but without any further explanatory statement, only with reference to an alleged free of charge and ultimately leaving

cases where content is deleted by a social network operator (usually Facebook) on the basis of the respective general terms and conditions. However, a reference to this case law alone would not suffice to implement Art. 17 (2) sentence 2 DSMD, since, on the one hand, it cannot always be assumed that a contract exists between the user and the service provider¹⁵³ and, on the other hand, this contract is not codified, which means that it would not satisfy the CJEU’s requirements for the correct implementation of a Directive.¹⁵⁴ In a case against the Netherlands, the European Court of Justice has clearly stated that:

“21 As regards the argument advanced by the Netherlands Government that, if the Netherlands legislation were interpreted in such a way as to ensure conformity with the Directive - a principle endorsed by the Hoge Raad der Nederlanden (Netherlands) - it would be possible in any event to remedy any disparity between the provisions of Netherlands legislation and those of the Directive, suffice it to note that, as the Advocate General explained in point 36 of his Opinion, even where the settled case-law of a Member State interprets the provisions of national law in a manner deemed to satisfy the requirements of a directive, that cannot achieve the clarity and precision needed to meet the requirement of legal certainty. That, moreover, is particularly true in the field of consumer protection.”¹⁵⁵

133 It can therefore only be questionable whether a claim to enforce limitations corresponding to Art. 6 (4) InfoSoc Directive against the service provider (not against the rightholders!) or, in general, a statutory, mandatory claim to upload content should be introduced. However, there are some reservations against such a broad subjective right which would go far beyond securing a procedural position: On the one hand, this would interfere with the privately autonomous design of the service providers (even though some network operators with a large market share such as Facebook, are subject to the indirect

open in the result; Higher Regional Court Munich MMR 2018, 760 para 20; Higher Regional Court Munich decision of 30 November 2018 – 24 W 1771/18, not published yet, p. 6; likewise, Higher Regional Court Stuttgart NJW-RR 2019, 35 para 20.

¹⁵³ Agreeing Hofmann (n 12) 1227; disagreeing Grisse (n 29) 899 who relies solemnly upon contract claims.

¹⁵⁴ Different opinion in Volkmann (n 12) 376, 382 paras 50 ff., who apparently wishes to allow contractual claims and the indirect third-party effect of fundamental rights to suffice – but this does not satisfy the requirements for transposition of the Directive.

¹⁵⁵ CJEU Case C-144/99 *Commission vs Netherlands* EU:C:2001:257.

binding of fundamental rights¹⁵⁶,¹⁵⁷ On the other hand, it could prejudice any regulations in specific (national) media laws, like specific access rules for users to gatekeepers within the Internet structure like social networks.

3. Protection of limitations by mandatory technology: Flagging

134 In addition to the subjective right to enforce limitations, limitations may be protected by the introduction of content “flagging” by users, which leads to the exclusion of corresponding content from automatic filtering pursuant to Art. 17 (4) (b) DSMD. The introduction of such a procedure which would be mandatory for service providers would also ensure that users could rely on the limitations to which they are entitled.¹⁵⁸

135 As explained above, however, the introduction of a mandatory “flagging” procedure in the Member States may conflict with the power of the EU Commission to define guidelines for the interpretation of Art. 17 (4) DSMD. Art. 17 (10) DSMD also refers expressly to the fundamental rights of users, and thus also to the limitations of Art. 17 (7) DSMD so that the Commission can also give concrete form to the limitations of the procedure under Art. 17 (4) (b) DSMD in the form of interpretation guidelines.

136 On the other hand, Art. 17 (7) (2) DSMD expressly requires measures for the implementation by the Member States (“shall ensure”) that users can enforce their rights. As explained above, this is made clear foremost by the explicit demand

for enforcement at state courts in Art. 17 (9) (2) DSMD. Without codified procedures to protect the limitations and the fundamental rights enshrined in them, however, these cannot be enforced effectively. It could also address the problem of blocking livestreams.¹⁵⁹ Moreover, as already mentioned, the Commission’s guidelines do not have binding effect vis-à-vis courts or authorities under Art. 17 (10) DSMD; they are not, like authorizations for Commission implementing Directives or the Commission implementing Regulations, legal acts with binding effect.¹⁶⁰ Rather, courts and authorities of the Member States must take into account the recommendations or guidelines, but may deviate from them. In contrast, Art. 17 (7) (2) DSMD requires a legally secured right for users to enforce their limitations; the mere inclusion of this right in guidelines would not sufficiently secure it and make it enforceable in any case. Therefore, despite the Commission’s authority to provide guidelines, the Member States must have the competence - and even the (constitutionally based) duty - to ensure the enforcement of the limitation, also and especially with the help of the described “flagging” procedures.

137 Vice versa, the liability for copyright infringement remains with users who mistakenly or even abusively mark their contents as covered by the limitations (“wrongful flagging”). As long as they did not err about legal provisions which can lead to the absence of fault,¹⁶¹ the liability already applies in case of negligence.¹⁶² Furthermore, in order to avoid abuses, such a user may be excluded from the complaint mechanism in the event of repeated and intended abuse.¹⁶³ However, it should also be desirable and part of the implementation to inform users about existing licenses for the platforms, and vice versa that an upload is not covered by a license.¹⁶⁴

¹⁵⁶ In that sense, the Federal Constitutional Court NVwZ 2019, 959 paras 1-25; in detail Benjamin Raue, “Meinungsfreiheit in sozialen Netzwerken” [2018] JZ 961; for a review of the different decisions of the Higher Regional Courts see Michael Beurskens, “Hate-Speech“ zwischen Lösungsrecht und Veröffentlichungspflicht” [2019] NJW 3418 ff.

¹⁵⁷ Spindler (n 127); Daniel Holznagel, “Put-back-Ansprüche gegen soziale Netzwerke: Quo Vadis” [2019] CR 518; Daniel Holznagel, “Overblocking durch User Generated Content (UGC) – Plattformen: Ansprüche der Nutzer auf Wiederherstellung oder Schadensersatz?” [2018] CR 369; Jörn Lüdemann, “Grundrechtliche Vorgaben für die Löschung von Beiträgen in sozialen Netzwerken” [2019] MMR 279; similar Hofmann (n 12) 1227.

¹⁵⁸ Statement of the German government from 15 April 2019: Draft Directive of the European Parliament and of the Council on copyright and related rights in the Digital Single Market and amending Directives 96/6/EC and 2001/29/EC – Statements [2019] 2016/0280(COD), 7986/19 ADD 1 REV 2; see also Dreier (n 28) 771, 778.

¹⁵⁹ Correctly Hofmann (n 12) 1228.

¹⁶⁰ See above n (131).

¹⁶¹ For the requirements, see Wolff, § 97 para 56 in Wandtke/Bullinger (eds), Praxiskommentar Urheberrecht (5th edn, CH Beck 2019), Spindler (n 47) § 97 paras 30 ff., Specht (n 41) § 97 para 78.

¹⁶² See also Hofmann, (n 12) 1228. For this reason, there is no need for a separate liability provision; other opinion Würtenberger/Freischem (n 87) 68.

¹⁶³ Similar Würtenberger/Freischem (n 87) 68.

¹⁶⁴ Correctly Hofmann, (n 12) 1227.

4. Design of procedural rights?

138 Art. 17 (9) DSMD provides some cornerstones for the design of the complaints procedure for users, for example that they must be “effective” and “expeditious” or that complaints must be dealt with immediately by a human being, and that extrajudicial redress procedures must be available which enable impartial occupancy without blocking access to state courts. Moreover, the Member States are free to design the procedures, which gives rise to a number of options. The procedural safeguarding of the rights of users are necessary in order to guarantee their fundamental right to a fair hearing, particularly in view of the aforementioned ruling of the CJEU in the UPC Telekabel case.¹⁶⁵

139 However, Member States must respect the complaints procedure laid down in Art. 17 (9) DSMD, which can only be triggered by a user’s complaint. In this context, the procedure developed by the German High Federal Court of Justice in the “Mallorca-Blogger” decision for violations of personality rights could be used: The provider forwards the complaint of a person affected (proprietor of the personality right) to the blogger (as infringer); if the blogger does not react within a reasonable period of time, the content is blocked. In the case of a reply from the blogger, the complainant is again invited to comment; if he fails to do so within a reasonable time, the content remains online.¹⁶⁶

140 Therefore, a transfer of these principles to the complaint’s procedure pursuant to Art. 17 (9) DSMD could be considered. After a complaint by a user, the rights owner would then be asked to comment; in the absence of a reaction within an extremely short period of time (e.g. 1-2 days), the content would then be put online again by assuming that the limitation is outweighed, or in the absence of legitimate interest in the proceedings by the rights owner. This would also be supported by Art. 17 (9) subparagraph 1 DSMD, which requires the right owner to justify the demand for blocking.

141 With regard to proceedings before state courts, the national legislator should provide for the quickest possible procedure in conformity with interim legal protection with short deadlines; the main proceedings could then be reserved for more complex questions of weighing limitations against existing copyrights.

165 See above n (52).

166 Federal Court of Justice GRUR 2012, 311 para 27.

5. Class action

142 The limitations in favor of users could also be strengthened by a right to file class actions or actions initiated by user/consumer associations.¹⁶⁷ However, Art. 17 (7), (9) DSMD is formulated as an individual right and is geared to a certain content of a user which could hardly be enforced in the context of a class action. Thus, a class action could only be aiming at a specific guideline or practice of the service providers, e.g. against specific upload filters used by a service provider which do not meet the conditions of Art. 17 (7), (9) DSMD.

V. The design and limitation of the legal consequences (damages)?

143 Finally, another option would refer to a limitation or exclusion of damages regarding users. However, this would contradict Art. 13 (1) Enforcement Directive¹⁶⁸ which provides for a full (“actual prejudice suffered”) claim for damages for the infringed rightholder. The Member States therefore have no room for maneuver here.

E. International private law

144 According to Art. 8 (1) Rome II Regulation¹⁶⁹ the *lex loci protectionis* principle applies to international copyright law.¹⁷⁰ However, the principle does not yet answer the question whether a national legal system is appointed according to *place of action* and *place where the harmful event occurred*. Concerning a copy or replication (regarding copyrights) it depends on where the copy was produced because that process is the actual commercial exploitation.¹⁷¹

Accordingly, for downloads it is widely accepted that the legal system of the country in which the copy

167 According to the proposal of *Specht*, not yet published.

168 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157/45 ff.

169 Regulation (EC) No 864/2007 of the European Parliament and of the Council 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199/40.

170 Regarding the term *Bach*, IPR Art. 8 ROM-II-VO para 1 in Spindler/Schuster (n 47); v. Welser, Vorb. §§ 120 ff. UrhG para 15 in Wandtke/Bullinger (n 164).

171 Federal Court of Justice GRUR 1965, 323, 325.

is made is the one to decide on possible claims, but also on the limits of the commercial exploitation.¹⁷²

145 For the right of communication to the public (or making available to the public), hence, for uploads the legal situation is more difficult: the actual utilization consists in the fact that access is possible for everyone so that on the one hand the act of communication to the public could be related to the place where the work is put on the internet,¹⁷³ or on the other hand to the place of retrieval (modified Bogsch theory)¹⁷⁴ – which due to the globality of the internet would then result in the application of every jurisdiction from which the content on the internet can be retrieved. Actually, the prevailing opinion tends to favour the last option – even though a decision by the Federal Court of Justice is yet to be passed.¹⁷⁵

172 Dreier, Vorb. §§ 120 ff. para 33 in Dreier/Schulze (eds), Urheberrechtsgesetz UrhG (6th edn, CH Beck 2018); Katzenberger/Metzger, Vor §§ 120 ff. Rn. 133, 143 in Schricker/Loewenheim (eds), Urheberrecht (5th edn, CH Beck 2017); Nordemann-Schiffel, Vor §§ 120 ff. Rn. 67 in Fromm/Nordemann (eds), Urheberrecht, (12th edn, Kohlhammer 2019); Gerald Spindler, “Morpheus, Napster & Co. - Die kollisionsrechtliche Behandlung von Urheberrechtsverletzungen im Internet“ in: Leible (ed), *Die Bedrohung des internationalen Privatrechts im Zeitalter der neuen Medien* (Richard Boorberg Verlag 2003), 155, 163 ff.; for the assessment when a reproduction is produced within the country see: Federal Court of Justice GRUR 1965, 323, 325; Federal Court of Justice, ZUM 2004, 371.

173 Jochen Dieselhorst, “Anwendbares Recht bei Internationalen Online-Diensten“ [1998] ZUM 293, 299 f.; Frank Koch, “Internationale Gerichtszuständigkeit und Internet“ [1999] CR 121, 123; Haimo Schack, “Zum auf grenzüberschreitende Sendevorgänge anwendbaren Urheberrecht“ [2003] IPRax 141, 142; Rolf Sack, “Das internationale Wettbewerbs- und Immaterialgüterrecht nach der EGBGB-Novelle“ [2000] WRP, 269, 277; Gerald Spindler, “Die kollisionsrechtliche Behandlung von Urheberrechtsverletzungen im Internet“ [2003] IPRax 412, 417.

174 See already Paul Katzenberger, “Urheberrechtsfragen der elektronischen Textkommunikation“ [1983] GRUR Int. 895, 916 f.; the Bogsch theory was developed by Arpad Bogsch, former Director General of WIPO, in connection with the right to broadcasting for satellite television, see on this matter Anette Kur, “Haftung für Rechtsverletzungen Dritter: Reformbedarf im europäischen IPR?“ [2011] WRP 971, 977; critical: Schwarz/Reber, § 21 paras 100 ff. with further references in Loewenheim (ed), *Handbuch des Urheberrechts* (2nd edn, CH Beck 2010).

175 See v. Welsler, Vor §§ 120 ff. UrhG para 19 in Wandtke/Bullinger (n 164); Katzenberger/Metzger (n 175) vor §§ 120 ff. UrhG para 142 f.; Hoeren (n 43) part 7.8 para 23; Hoeren, part 14 paras 5 f. in: Kilian/Heussen (eds), *Computerrechts-*

146 Since, according to Art. 17 (1) DSMD, the service providers themselves violate the right of communication to the public, every jurisdiction is applicable in which the content uploaded by users can be retrieved. This in turn creates a European “patchwork” in the event of divergent implementation in the Member States: If, for example, Germany introduces a “flagging” procedure but France does not, this procedure would not apply to French users who want to upload content to a German platform, since the flagging procedure would not intervene in France. Service providers may therefore start to use suitable geoblocking techniques. These geo-localizations are mostly known from the field of gambling on the internet and allow precise localizations up to a few kilometers, in combination with other methods, such as mobile phone tracking, even up to a few meters.¹⁷⁶ However, these measures can be circumvented by using anonymization services, virtual private networks (VPNs) or proxy servers, which are set up at the desired location, unless further positioning services (such as mobile phone tracking) are linked to them.¹⁷⁷ However, since

Handbuch (34 edn, CH Beck 2018); see jurisdiction on this matter: Regional Court Hamburg, BeckRS 2008, 23065, that applied § 19a UrhG in a case in which a company based in the USA had made thumbnails of copyrighted images publicly available on the Internet; like this already Gerald Spindler, “Die kollisionsrechtliche Behandlung von Urheberrechtsverletzungen im Internet“ [2003] IPRax 412, 418 ff. with further references.

176 On this matter, Thomas Hoeren, “Geolokalisation und Glückspielrecht“ [2008] ZfWG 311, 312 f.; Critical to the technical feasibility of sufficiently precise geolocation in the context of gambling law Higher Administrative Court Lüneburg NVwZ 2009, 1241, 1243; equally Administrative Court Berlin BeckRS 2012, 48575; other opinion Administrative Court Düsseldorf BeckRS 2011, 53037, which considers the available methods to be sufficient under gambling law; equally Higher Administrative Court Münster BeckRS 2010, 51049; for further references on jurisdiction see Michael Winkelmüller und Hans Wolfram Kessler, “Territorialisierung von Internet-Angeboten – Technische Möglichkeiten, völker-, wirtschaftsverwaltungs- und ordnungsrechtliche Aspekte“ [2009] GewArch 181, 182; critical to geoblocking: Ansgar Ohly, “Geoblocking zwischen Wirtschafts-, Kultur-, Verbraucher- und Europapolitik“ [2015] ZUM 942; see also for other areas of application and services Thomas Hoeren, “Zoning und Geolocation - Technische Ansätze zu einer Reterritorialisierung des Internet“ [2007] MMR 3, 3 f.

177 Detailed on this matter, Aileen Prill, *Webradio-Streamripping: Eine neue Form der Musikpiraterie?* (1st edn, Peter Lang 2013) 37 ff. with further proof to the technology; see also Hoeren, (n 179) 311, 311 f.; Hoeren, (n 179) 3, 6; for anonymisation services see Marco Rau and Martin Behrens, “Catch me if you can ... Anonymisierungsdienste und die

geolocalization requires the processing of personal data by identifying the origin of IP addresses and requests, at least pseudonymization is inevitable. The federal and the state commissioners for data protection consider the use of only the first 4 bytes for geolocalization to be sufficient for IP addresses according to the Internet protocol IPv6.¹⁷⁸

147 In this context, the so-called Geoblocking Regulation¹⁷⁹ does not prevent the application of these methods: according to Art. 1 (5) Geoblocking Regulation, it does not apply to copyright law; therefore, actions and tools used by service providers to exclude users from other countries are permitted.

148 The new Portability Regulation¹⁸⁰ does not change this either, since it only applies to consumers by regulating a legal fiction for them in Art. 4. As a result, the rights of use for certain online content are limited to the Member State of residence, regardless of where the user actually resides.¹⁸¹ However, it

does not interfere with the obligations of service providers under Art. 17 DSMD.

Haftung für mittelbare Rechtsverletzungen“ [2009] K&R 766 ff.

178 See resolution of the 82nd Conference of Data Protection Supervisors of the Federal Government and the Federal States on 28-29 September 2011 in Munich, p 2, accessible at: <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entscheidungssammlung/DSBundLaender/82DSK_IPv6.pdf;jsessionid=0E81AF686CF133FA9272C5BFF4342070.1_cid354?__blob=publicationFile> (accessed 28 October 2019); differentiating depending on the localisation purpose Ulrich Kühn, “Geolokalisierung mit anonymisierten IP-Adressen“ [2009] DuD 747, 751.

179 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers’ nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, OJ L 60 I/1 ff.

180 Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ L 168/1.

181 Nordemann-Schiffel (n 175) Art. 4 PortVO, para 1; v. Welser (n 164) Vor §§ 120 ff. UrhG para 19; for detailed on the new Portability Regulation see Johann Heyde, “Die Portabilitätsverordnung – Auswirkungen auf die Lizenzverträge“ [2017] ZUM 712.

F. Copyright law obligations of platforms outside the scope of the DSMD

149 If a platform or service provider does not fall within the definition of Art. 2 (6) DSMD, Art. 17 DSMD shall (of course) not apply¹⁸² with the consequence that Art. 14 ECD remains applicable, as well as the case-law of the CJEU outlined briefly above. If the CJEU¹⁸³ qualifies platforms that place advertisements in connection with user-generated content and carry out further structuring as perpetrators (infringers) themselves with regard to the right of making available to the public (Art. 3 InfoSoc Directive), these platforms which fall outside the scope of Art. 2 (6) DSMD would nevertheless be subject to comparable obligations. Should the CJEU extend the infringement to platforms and thus assume a liability by a breach of duty to care in the YouTube/Uploaded proceedings, the existing German *Stoererhaftung*, which accepts obligations only after knowledge, would in fact be void.¹⁸⁴

150 From a dogmatic point of view, it remains unclear whether Art. 17 DSMD is then to be regarded as the exclusive regulation for Art. 3 InfoSoc Directive,¹⁸⁵ so that an extended application of Art. 3 InfoSoc Directive would also be excluded if the scope of Art. 17 DSMD is not opened up. In other words, it is conceivable that the CJEU reaches the conclusion that Art. 3 InfoSoc Directive applies also to platforms with a non-commercial purpose etc. – which are now excluded from Art. 17 DSMD by means of definition of Art. 2 Nr. 6 DSMD. However, if Art. 17 DSMD is exclusive the CJEU case law on the right to make available to the public (with its extensions) would

not be applicable any more. The DSMD does not contain any clear provisions on this subject. Rather, recital 64 DSMD states that Art. 17 DSMD should not

182 This does not apply to start-ups under Art. 17 (6) DSMD, as they are still subject to the regime of Art. 17 of the DSMD, but with the obligations reduced in Art. 17 (6) in conjunction with Art. 4 (c) of the DSMD. In this context, it is not clear to what extent the provisions in recital 66, according to which the national remedies should continue to apply - hence also the German “*Stoererhaftung*“.

183 See above n 7 f.

184 Stieper (n 10) 211, 216 f.; High Federal Court of Justice GRUR 2018, 1132, 1139, 1141 with comments by *Ohly*.

185 For the various interpretation attempts of the relationship between Art. 17 DSMD and Art. 3 InfoSoc Directive see Husovec/Quintais (n 139) who regard Art. 17 itself as a right sui generis.

prejudice the application of Art. 3 InfoSoc Directive. Thus recital 64 sentence 3 of DSMD reads as follows:

- 151** “This does not affect the concept of communication to the public or of making available to the public elsewhere under Union law, nor does it affect the possible application of Art. 3(1) and (2) of Directive 2001/29/EC to other service providers using copyright-protected content.”
- 152** However, the explicit regulation of liability privileges and the exception, e.g. for startups (Art. 17 (6) DSMD), indicate that for other platforms outside the DSMD (e.g. non-commercial platforms, cloud services, etc.) no stricter liability (due to an extensive interpretation of Art. 3 of the InfoSoc Directive) can intervene, as otherwise the regulations or privileges would run nowhere. Even if Art. 3 InfoSoc Directive should be applied extensively by the CJEU (regardless of the DSMD), users should still benefit from an analogous application of the procedural guarantees to safeguard fundamental rights.

G. Conclusion

- 153** The analysis showed the complex triangle between users, service providers, and rightholders enshrined in Art. 17 – which is just a part of the general problem of balancing the rights in this multilateral relationship. It seems impossible to safeguard all rights at the same time so that the fundamental constitutional problem consists in striking a fair balance between those rights. Whereas Art. 17 (4) b) DSMD respects that there is no proactive obligation of providers to monitor their platforms, thus establishing a more or less adequate balance of rights, if at the same time flagging procedures etc. are available for users, the same is unfortunately not true for the obligations to check the platform in general with regard to content that has to be licensed (Art. 17 (1) DSMD). Moreover, national legislators should carefully implement subjective rights and procedures for users in order to safeguard their constitutional rights.