2. The Relevant EU Legal Framework for Online Content Dissemination

In order to start with the presentation of the existing legal framework for the dissemination of online content, which is also the starting point for enforcement measures, a number of provisions[29] and legal acts in the areas of fundamental rights as well as in primary and secondary law of the European Union needs to be considered. However, as the study focuses on regulatory issues at the EU level in order to identify possible improvements, the framework of international law will not be presented here.[30] In the online context, coordination, support and supplementary measures of the EU also play a role, particularly in the context of the direct involvement of third-country service providers.

2.1. Fundamental Rights

Fundamental rights[31] as the highest legal assets within democratic states, both in their (subjective) expression as defensive rights of natural and legal persons and partly as (objective) guarantees, must be safeguarded as the basis of every legal framework and in every legislative and regulatory activity. In some cases, they can oblige the states bound to them to (certain) actions in order to counteract (also actively regulating) existing circumstances that cannot be reconciled with fundamental and human rights and to eliminate existing impairments.

The online dissemination of content has a number of links to fundamental and human rights, which mirror the participation of different stakeholders with different interests. This includes above all the users who access the services of online service providers. They are the primary recipi-

29 The provisions in particular relevant in the context of this study are listed or reprinted in the Online Annex, available at www.nomos-shop.de/44382.

30 Cf. on international aspects *Ukrow*, Zuständigkeit der Landesmedienanstalten/KJM für ausländische Anbieter; and *Cappello (ed.)*, Media law enforcement without frontiers, IRIS Special 2018-2.

31 Fundamental rights relevant in the context of this study are listed in the Online Annex, available at www.nomos-shop.de/44382, I.

ents who consume the content, and in some cases they are also active participants in the online content of third parties appearing as actors or as real persons. In both cases, human dignity and the protection of minors have key importance that needs to be taken into account by online content providers in order to comply with fundamental rights. These high-ranking values regularly run in parallel with the public interests that guide, and must guide, state activities. With regard to the latter group of users, personal rights aspects are also to take into account, namely in form of data protection and the protection of private life. While they can refer to their right to information as recipients, on the other hand, the users themselves are increasingly becoming content creators who disseminate their own contributions via intermediaries and thus can rely on the right to freedom of expression. The way in which they create and disseminate content as well as the extent to which they allow specific content to be disseminated, has an impact on how to categorise the providers. In particular, apart from being able to rely "only" on the freedom of expression they can likely also rely on the freedom of the media, which can have relevance, as within the framework of media freedom other criteria might be applied in light of the role of the media as a public watchdog. It is precisely this freedom of the media as well as the right to property, particularly with regard to intellectual property, that content creators regularly invoke when their content is disseminated via their own platforms or those of intermediaries. They have an interest in their content also being protected online. Finally, intermediaries who offer their services out of economic interest are protected by fundamental rights in terms of their freedom to conduct a business and their right to property.

To what extent and when these fundamental rights oblige the EU at Union law level and the states at national level to take active action will be examined below.

2.1.1. Fundamental Rights Sources: EU Charter, European Convention on Human Rights and National Constitutional Law

Although provided for in the Treaty on European Union (TEU)[32], the Union has not yet acceded to the European Convention on Human Rights (ECHR)[33]. Nevertheless, the ECHR has an important impact on the EU in two respects: On the one hand, the Member States as Convention States are bound to the ECHR as a source of international law, also in the implementation of Union law, which at the same time means that the Member States are guarantors of measures taken by the Union. On the other hand, even after the adoption of the Charter of Fundamental Rights of the European Union (CFR)[34], the ECHR is still one of the most relevant legal references within Union law.[35] The CJEU recognises in its decisions that "the principles on which the European Convention for the Protection of Human Rights and Fundamental Freedoms is based must be taken into consideration in community law"[36], and it states that "fundamental rights form an integral part of the general principles of the law, the observance of which is ensured by the Court. In safeguarding those rights, the Court has to look to the constitutional traditions common to the Member States, so that measures which are incompatible with the fundamental rights recognized by the constitutions of those States may not find acceptance in the Community"[37]. This means that the CJEU therefore incorporates both the norms of the ECHR and the case law of the European Court of Human Rights (ECtHR) into its decisions, in particular within the framework of the justification of infringements of fundamental rights guaranteed in the CFR.[38] This applies in particular due to the equality clause contained in Art. 52 para. 3 CFR, which states that, insofar as the CFR contains rights

32 Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390.

33 The European Convention on Human Rights, as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.

34 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.

35 *Kingreen*, in: Calliess/Ruffert, Art. 6 TEU para. 20 et seq.

36 CJEU, judgement of 15.5.1986, C-222/84, *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary*, para. 18.

37 CJEU, judgement of 13.7.1989, C-5/88, *Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft*, para. 17.

38 CJEU, judgement of 26.6.1997, C-368/95, *Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH v Heinrich Bauer Verlag*, para. 26.

which correspond to rights guaranteed by ECHR, the meaning and scope of those rights shall be the same as those laid down by the said Convention. However, Art. 52 para. 3 also states that "[t]his provision shall not prevent Union law providing more extensive protection", which, in principle, could lead to divergences in jurisprudence. On the other hand, the ECtHR also assumes that an equivalent level of protection of fundamental rights is guaranteed in the Union[39], so that the application of different standards is rather unlikely.[40]

With regard to the relationship between the ECHR and the CFR, on the one hand, and national constitutional law, on the other, which should not be the subject of consideration of the present report, it must be said that these three levels of protection of fundamental rights, in principle, complement each other cumulatively.[41] This also corresponds to Art. 53 CFR on the level of protection of the CFR, which states that "nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognized inter alia by the Member States' constitutions".

On the part of Union law, however, the fundamental primacy of Union law, which is expressed in Art. 51 para. 1 CFR, must also be observed. The fundamental primacy of the fundamental rights of the Union over those of the national constitutions results from the transfer of sovereign rights to the Union, which is not changed by the regulation of Art. 53 CFR.[42] Therefore, it is settled jurisprudence of the CJEU that rules of national law, even of a constitutional order, cannot be allowed to undermine the effectiveness of EU law on the territory of that State.[43] Although the CJEU is guided by the constitutional traditions common to the Member States and the principles derived from the ECHR when interpreting the CFR and developing jurisdictional principles[44], conflicts are nevertheless conceivable. Such conflicts would then have to be resolved in favour of Union law, but this does not mean that far-reaching constitutional protection per se would be superseded.[45]

---

39 ECtHR, judgement of 30.6.2005, no. 45036/98.
40 *Kingreen*, in: Calliess/Ruffert, Art. 6 TEU para. 23.
41 *Ladenburger/Vondung*, in: Stern/Sachs, Art. 51 para. 39 et seq.
42 *Everling*, in: EuZW 8/2003, p. 225.
43 CJEU, judgement of 26.2.2013, C-399/11, *Stefano Melloni v Ministerio Fiscal*, para. 59 with further references.
44 *Everling*, in: EuZW 8/2003, p. 225.
45 *Ladenburger/Vondung*, in: Stern/Sachs, Art. 51 para. 39, 40.

This applies in particular to positive state protection obligations which can arise from the constitutions of the Member States – also against the background of Art. 51 para. 1 sentence 2 CFR. This is indicated in particular by considerations that can be drawn from the CJEU's case law on fundamental freedom. In the *Commission/France* case[46] the CJEU clarified not only that the prohibition rules derived from fundamental freedoms prohibit measures which are attributable to a Member State and which themselves create restrictions on trade between the Member States; it stated also that these rules can apply where a Member State abstains from adopting the measures required in order to deal with obstacles to the fundamental freedoms (in this case the free movement of goods) which are not caused by the State.[47] The fundamental freedoms may be affected, in the same way as they may be affected by an act of a Member State, by a Member State's failure to act, or its failure to take sufficient measures to remove obstacles to a fundamental freedom caused, in particular, by acts of private individuals within its territory which are directed against the activity protected by the fundamental freedom. Thus, the fundamental freedoms may oblige Member States not only to remedy certain infringements but also to take all necessary and appropriate measures, taking into account the frequency and seriousness of such infringements, for example by private individuals, to ensure that those fundamental freedoms are respected in their territory, unless they can prove that their action would have consequences for public policy which they could not overcome by their means. However, the Member States have a considerable margin of appreciation with regard to the concrete measures to be taken, which cannot be imposed by the Union[48] – probably outside of cases where there is no other appropriate solution.

46 CJEU, judgement of 9.12.1997, C-265/95, *Commission of the European Communities v French Republic*. Cf. on this already *Ukrow*, Zur Zuständigkeit der Landesmedienanstalten/KJM für ausländische Anbieter.

47 CJEU, ibid., para. 30.

48 Ibid., para. 33 et seq.

2.1.2. Relevant Fundamental Rights

2.1.2.1. Human Dignity

Human dignity is inviolable. It must be respected and protected. This overriding principle and fundament of all other fundamental rights can be found in Art. 1 CFR. Although the ECHR does not explicitly mention human dignity, the ECtHR assumes that the principle of respect for human dignity underlies all Convention guarantees[49] and that "[t]he very essence of the Convention is respect for human dignity and human freedom"[50]. Human dignity is both a fundamental right with subjective guarantee content and a principle under objective law.

The institutions, bodies, offices and agencies of the Union are bound by fundamental rights within the meaning of Art. 51 para. 1 CFR, in compliance with the principle of subsidiarity, as well as the Member States when they implement Union law. Private individuals, on the contrary, are not covered by the scope.[51] However, it has always been difficult to concretise the content of human dignity or even to find a definition.[52] Rather, in practice, it is treated by the CJEU[53] and the ECtHR as a kind of general clause or basic standard, which can be applied where a more sector-specific fundamental right is not applicable.[54] Without going into the historical development and its further development in the jurisprudence of the European courts in greater depth, it can be stated here that at least the minimum core of human dignity consists in the fact that every human being possesses an intrinsic worth, merely by being human, which should be recognised and respected by others. Recognising the intrinsic worth of the individual requires that the state should be seen to exist for the sake of the individual human being, and not vice versa.[55]

---

49 ECtHR, judgement of 11.7.2002, no. 28957/95, para. 90.
50 ECtHR, judgement of 29.4.2002, no. 2346/02, para. 65.
51 Cf. *Classen*, EuR 39(3), 2004, pp. 416, 429 et seq.; *Jaensch*, Die unmittelbare Drittwirkung der Grundfreiheiten, pp. 186 et seq.; for developments towards a horizontal impact of fundamental freedoms see *Schepel*, in: ELJ 18(2), 2012, p. 177, 192 et seq.
52 Cf. for an overview on the different approaches *von Schwichow*, Die Menschenwürde in der EMRK, pp. 13 et seq.
53 Cf., e.g., CJEU, judgement of 9.10.2001, C-377/98, *Kingdom of the Netherlands v European Parliament and Council of the European Union*, para. 70.
54 *Höfling/Kempny*, in: Stern/Sachs, Art. 1 para. 9.
55 In this regard *McCrudden*, in: EJIL 19(4), 2008, p. 655, 655 et seq.

As the wording of Art. 1 CFR unequivocally shows, human dignity is inviolable and thus not subject to any restrictions or justification.[56] On the other hand, the protection of human dignity can be a suitable objective within the framework of the restriction of fundamental freedoms. With regard to human dignity and the restriction of the freedom to provide services, the CJEU explained this in its *Omega*[57] ruling:

> *"There can therefore be no doubt that the objective of protecting human dignity is compatible with Community law, it being immaterial in that respect that, in Germany, the principle of respect for human dignity has a particular status as an independent fundamental right. Since both the Community and its Member States are required to respect fundamental rights, the protection of those rights is a legitimate interest which, in principle, justifies a restriction of the obligations imposed by Community law, even under a fundamental freedom guaranteed by the Treaty such as the freedom to provide services."*[58]

Especially the latter decision of the CJEU shows that it is not excluded that the assessment of human dignity as a protection objective in connection with the restriction of fundamental freedoms is based on a national understanding of this fundamental right[59] and not on an understanding under Union law.[60]

In the area of online content, there are many conceivable possibilities for violating human dignity. This applies in particular to audiovisual content that contains pornography or depictions of violence.[61] It also applies in the field of non-fictional depictions of violence, in which the effect of violence on the body of a person against his will can make him "an object" and therefore could come into conflict with human dignity. Examples include execution videos of terrorist organisations or so-called "snuff videos", for which the Internet is the most common means of dissemination. In fic-

56 *Höfling/Kempny*, in: Stern/Sachs, Art. 1 para. 27.

57 CJEU, judgement of 14.10.2004, C-36/02, *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn*. This case was about a prohibition of an installation known as a "laserdrome", normally used for the practice of "laser sport" in which the players shoot each other playfully with laser guns.

58 Ibid., para. 34, 35.

59 The so-called "laserdromes" were not prohibited in other Member States which was one of the arguments of the claimant.

60 In this regard also *McCrudden*, in: EJIL 19(4), 2008, p. 655, 710.

61 Cf. on the (also media-political) discussion already *Schulz*, in: M&K 48(3), 2000, p. 354, 354 et seq.

tional media content, on the other hand, in which all the actors voluntarily agree to the actions depicted, it will regularly not be possible to affirm a violation of human dignity through the production or publication of the content, even if these depictions are particularly obscene or glorify violence. In the latter cases, however, the human dignity of the viewer may be violated if the identification with the portrayed person violates his dignity, whereby the portrayal cannot escape him (because it may surprise him due to a lack of appropriate labelling).[62] Moreover, in principle, situations are also conceivable in the field of fictional content that must be subsumed under human dignity because, for example, the subjects acting in the video are not at all in a position – whether due to mental, physical or age-related incapacity to consent – to grasp what is portrayed and its effects in their entirety and thus cannot effectively consent to the production and/or publication of the content.[63]

2.1.2.2. Rights of the Child and Protection of Minors

The rights of children play a special role in the CFR. In accordance with the United Nations Convention on the Rights of the Child[64], Art. 24 CFR considers children to be independent holders of fundamental rights. This separate establishment in separate provisions outside of Art. 6 CFR shows that the CFR does not regard children as a union with their parents but rather treats them as independent rights holders.[65] Art. 24 para. 1 CFR guarantees that children shall have the right to such protection and care as it is necessary for their well-being (as a subjective right of participation and protection vis-à-vis the EU institutions and the Member States) and that they may express their views freely. Moreover, such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. According to Art. 24 para. 2 CFR, in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.

---

62 *Schulz*, in: M&K 48(3), 2000, p. 354, 366.

63 Cf. extensively on this *Dörr/Cole*, Big Brother und die Menschenwürde, p. 82; *Dörr/Cole*, in: K&R 8/2000, p. 369, 377; *Cole*, in: HK-RStV, § 3 and § 41.

64 Convention on the Rights of the Child, New York, 20.11.1989, available at https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=en.

65 Cf. on this *Steindorff-Classen*, in: EuR 46(1), 2011, p. 19, 31.

As a value decision in favour of the welfare of the child, Art. 24 primarily contains an objective legal component as well as a connecting factor for the target-oriented restriction of other fundamental rights and a requirement for the welfare-oriented interpretation of other laws – including those on a national level.[66] Art. 24 therefore rather contains guidance for the interpretation of secondary law[67], while the CJEU is very cautious in deriving individual protective rights arising from it[68]. "Protection" within the meaning of Art. 24 para. 1 sentence 1 CFR means that children (which also includes youth) are to be protected from anything that could endanger their well-being, i.e., that could impair their health, safety, physical, mental or moral development.[69] This provision can, therefore, be invoked as a connecting factor where fundamental rights of third parties are affected by rules designed to protect the development of minors. Art. 24 para. 1 sentence 2 CFR has, in addition to Art. 11 CFR, less significance against a background of fundamental rights, since children also fall within the personal scope of protection of freedom of expression. Therefore, Art. 24 para. 1 sentence 2 CFR underlines at this point only once more that children are to be seen as independent personalities by emphasising their right to free speech.[70]

Although Art. 24 CFR is based on the United Nations Convention on the Rights of the Child, the provision, unlike Art. 17 of the Convention, contains no specific rules on the protection of minors from harmful media or in the media environment. Thus, the protection of minors in the media has so far played no role in the fundamental case law of the CJEU. It is rather – a small number of – judgements on the AVMSD and partly also on the ECD that have dealt with this issue. Protection of minors in the media continues to be an objective that follows to a large extent[71] from national constitutional law and is therefore essentially left to the discretion of the Member States in its implementation.[72]

---

66 *Ennuschat*, in: Stern/Sachs, Art. 24, para. 6.
67 Cf. on this CJEU, judgement of 6.12.2012, joint cases C-356/11 and C-357/11, *O and S v Maahanmuuttovirasto and Maahanmuuttovirasto v L*.
68 Cf., e.g., CJEU, judgement of 8.11.2012, C-40/11, *Yoshikazu Iida v Stadt Ulm*.
69 *Ennuschat*, in: Stern/Sachs, Art. 24, para. 8, 9.
70 In this regard also *Ennuschat*, in: Stern/Sachs, Art. 24, para. 13.
71 Although there are now links at secondary law level (e.g. Art. 6a AVMSD).
72 Cf. on national case law regarding the protection of minors in the media *Cappello (ed.)*, The protection of minors in a converged media environment, IRIS plus 2015-1, pp. 53 et seq.

Although the protection of minors is not expressly regulated in the ECHR, the ECtHR repeatedly emphasises in its judgments the special need for protection of minors. In the context of this study, two judgments of the ECtHR are particularly relevant, since they are related to media or digital content. The *Söderman case* concerned the attempted covert filming of a 14-year-old girl by her stepfather while she was naked and her complaint that the Swedish legal system, which at the time did not prohibit filming without someone's consent, had not protected her against the violation of her personal integrity. In its judgment, the ECtHR assumed an infringement of Art. 8 ECHR pointing out that "the circumstances were aggravated by the fact that the applicant was a minor"[73]. While in this case the ECtHR did not also have to deal with the publication of the video material (this had not happened), the case *K.U. v. Finland* took place in the online environment. This case concerned a personal ad with sexual content that had been posted on a dating website on the Internet on behalf of a twelve-year-old boy. Neither the Finnish legislation in force at that time nor the police, nor the Finnish courts were able to oblige the Internet service provider to identify the person who placed the advertisement. In particular, the Internet service provider refused to identify the responsible person because this would constitute a breach of his duty of confidentiality. In this case the ECtHR held an infringement of Art. 8 ECHR too and highlighted the notion of private life, given the potential threat to the boy's physical and mental welfare at his vulnerable age.[74] The Court considered that the posting of the Internet advertisement about the applicant had been a criminal act that had resulted in a minor having been a target for paedophiles. It recalled that such conduct called for a criminal-law response and that effective deterrence had to be reinforced through adequate investigation and prosecution. Moreover, children and other vulnerable individuals were entitled to protection by the state from such grave interferences with their private life. According to the ECtHR, the Finnish Government could not argue that there had been no opportunity to put in place a system to protect children from being targeted by paedophiles via the Internet because it had been well-known that the Internet, precisely because of its anonymous character, could be used for criminal purposes. The widespread problem of child sexual abuse had also become well-known. Moreover, according to the ECtHR, the legislature should have provided a framework for reconciling the confidentiality of Internet services with the

73 ECtHR, judgement of 12.11.2013, no. 5786/08, para. 86.
74 ECtHR, judgement of 2.12.2008, no. 2872/02, para. 41.

prevention of disorder or crime, and the protection of the rights and freedoms of others.[75] Two other decisions are also noteworthy in this regard. In the first, the ECtHR stated that there was no unlawful restriction of freedom of expression when the Member States took measures against the (admonished) exhibition of Internet child pornography.[76] In the second, the ECtHR ruled that the national provisions with regard to fines and applicable procedures for the protection of minors must comply with the principle of proportionality[77].

2.1.2.3. Respect for Private and Family Life

The CFR, unlike many national constitutions and the ECHR, explicitly guarantees the right to the protection of personal data. In the context of the genesis of Art. 8 CFR the provisions of the Data Protection Directive[78] at that time were reproduced, which were taken over essentially also in the now valid General Data Protection Regulation (GDPR). According to this, everyone has the right to the protection of personal data concerning him or her (para. 1) as well as the right of access to data which has been collected concerning him or her, and the right to have it rectified (para. 2). Furthermore, Art. 8 para. 2 CFR lays down some important principles to take into account while processing personal data: personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Finally, according to Art. 8 para. 3, compliance with these rules shall be subject to control by an independent authority.

This results in a mainly subjective-legal component, according to which the individual has a right to the protection of his or her personal data in compliance with the requirements specified in Art. 8 CFR. Provisions,

---

75 ECtHR, judgement of 2.12.2008, no. 2872/02, para. 43 et seq.

76 ECtHR, judgement of 10.5.2011, no. 1685/10. The case concerned an artist (applicant) who exhibited her work "the Virgin-Whore Church" in an art gallery in Helsinki opened to the public. The work included hundreds of photographs of teenage girls or otherwise very young women in sexual poses and acts. The pictures had been downloaded from free Internet pages and some of them were extremely violent or degrading.

77 ECtHR, judgement of 21.7.2011, nos. 32181/04 and 35122/05.

78 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31–50.

inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter.[79] The addressees of this fundamental right are the institutions and bodies of the EU and the Member States when implementing Union law (Art. 51 para. 1 CFR). Against the background of the increased importance of data protection, especially in the relationship between private individuals, the direct third-party effect of the fundamental right is also discussed.[80] The CJEU takes this matter into account insofar as it transfers the principles following from Art. 8 CFR to the interpretation of the data protection rules of the EU.[81] The justification of infringements takes place – beside the special limitation clause of Art. 8 para. 2 sentence 1 CFR, stating that personal data are to be processed only in good faith for fixed purposes and on the basis of a legally fixed basis – according to the horizontally applicable test of Art. 52 para. 1 CFR (see already above).[82]

The processing of (personal) data is omnipresent on the Internet – whether this takes place via the content itself (through processing of data of persons portrayed in the respective content) or is part of offer structures on the Internet (cookies, personalised advertising, data and address trading, etc.).[83] Both content providers[84] and distributors must therefore comply with data protection rules that result from the interests of those affected and are protected by fundamental rights. These specifications are comprehensively codified at the level of EU secondary law with the GDPR, which also provides for a differentiated sanction framework, which is used by the national authorities set up under the law of the Member States. In addition, thereby a further element of Art. 8 CFR is addressed, which was a

79 CJEU, judgement of 6.10. 2015, C-362/14, *Maximillian Schrems v Data Protection Commissioner*, para. 38; cf. also judgements of 20.5.2003, joint cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*, para. 68; of 14.5.2014, C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 68; of 11.12.2014, C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, para. 29.

80 Cf. on this *Streinz/Michl*, EuZW 2011, p. 384, 385.

81 CJEU, *Google Spain v AEPD*, supra (fn. 79), para. 68

82 CJEU, judgement of 9.11.2010, joint cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, para. 53.

83 Cf. on this in detail para. 2.4.3.2.

84 On the special characteristics of journalistic services against the background of media privileges, cf. in more detail at para. 2.4.3.1.

previously unusual specific laying down of separate data protection rights in a fundamental rights catalogue and therefore deserves to be mentioned also in the context of this study.

The CJEU underlined "that the question of compliance has to be subject to control by an independent authority, as follows from primary law of the EU and, in particular, from Art. 8 para. 3 CFR and Art 16 para. 2 TFEU."[85]. It is necessary for the competent supervisory authorities to be independent so as to enable them to carry out their tasks without external interference. Such independence shall preclude, inter alia, any direct or indirect instruction or any other form of external influence which might guide their decisions and call into question the fulfilment of their tasks by the said authorities.[86] With this provision, therefore, an organisational regulation is anchored constitutionally, which is more closely designed in the provisions of Art. 51 et seq. GDPR and implemented accordingly by the Member States.

Regarding the ECHR, Art. 8 para. 1 sets out the precise rights which are to be guaranteed to an individual by the state – the right to respect for private life, family life, home and correspondence. According to the ECtHR, private life is a broad concept that is incapable of an exhaustive definition.[87] The ECHR, however, also subsumes the protection of data under this term if they have a connection to private life.[88] For example, the ECHR has recently clarified, in the context of the monitoring of employees at their workplace, that, even if the private use of company means of communication is prohibited, the employer does not have the right to monitor the use of the means of communication unrestrictedly and at his discretion.[89] Art. 8 ECHR is also primarily a right of defence against state interference. However, the ECtHR also recognises that the obligations included in Art. 8 may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.[90] Corresponding to Art. 51 para. 1 CFR, Art. 8 para. 2 ECHR states that the rights guaranteed by Art. 8 para. 1 ECHR are not absolute and that it may be acceptable for public authorities to interfere under certain circumstances. Only interferences which are in accordance with

85 CJEU, judgement of 8.4.2014, C-288/12, *European Commission v Hungary*, para. 47.
86 Ibid., para. 51.
87 ECtHR, judgement of 25.3.1993, no. 13134/87, para. 36.
88 ECtHR, judgement of 29.4.2013, no. 24029/07.
89 ECtHR, judgement of 5.9.2017, no. 61496/08.
90 ECtHR, judgement of 12.11.2013, no. 5786/08, para. 78.

law and necessary in a democratic society in pursuit of one or more of the legitimate aims listed in Art. 8 para. 2 CFR will be considered to be an acceptable limitation by the state of an individual's rights. However, the ECtHR leaves to the Convention States a margin of appreciation. This margin is given both to the domestic legislator and to the (judicial) bodies that are called upon to interpret and apply the laws in force. The scope of this margin of appreciation will differ according to the context, and it has been held, for example, to be particularly wide in areas such as child protection. Here, the Court has recognised that there is diversity in approaches to childcare and state intervention into the family among Convention States. Accordingly, it allows States a measure of discretion when examining such cases under the ECHR.[91]

2.1.2.4. Freedom of Expression and the Media

Art. 10 ECHR guarantees that everyone has the right to freedom of expression, which includes the freedom to hold an opinion and to receive and impart information. However, the ECHR does not guarantee these freedoms indefinitely but accepts that free speech is also associated with duties and responsibilities. In this respect, Art. 10 para. 2 allows limitations if they are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary. Both at the level of the scope of protection and at the level of justification, the ECHR contains relatively abstract and broadly defined rules which can only be (or become) defined by the case-law of the ECtHR. Accordingly, the ECtHR also promotes a broad understanding of Art. 10 ECHR, which covers all communication behaviour irrespective of whether it is an individual expression of opinion or the mass media dissemination of information. Differentiation between different media manifestations, which is also influenced by the significance of the respective means of communication for the public opinion-

91 ECtHR, judgement of 27.11.1992, no. 13441/87; cf. on this in detail *Kilkelly*, Human rights handbook No. 1. This margin of appreciation applies also in the field of the protection of individual's data; cf. ECtHR, judgement of 5.9.2017, no. 61496/08, para. 112.

building, does not initially take place at the level of the scope of protection but rather at the level of justification of restrictions and the degree of state duty to protect to be guaranteed. Online content is, therefore, generally covered by this broad scope, including content that is insulting or shocking in nature.[92] Interventions in this comprehensively understood area of protection are conceivable in many ways and range from preventing or making more difficult the reception/accessibility of such services or individual contents to merely labelling them. Thus, the deletion of a comment representing "hate speech"[93] intervenes in the freedom of expression or freedom of the media just as much as a blocking obligation with regard to a news platform against an access provider.

At the level of justification, however, which initially demands an urgent social need for the use of the barriers under Art. 10 para. 2 ECHR, which must be asserted by the state appropriately, carefully and in good faith and presented convincingly[94], differentiation takes place. For example, the signatory states have a certain margin of appreciation when assessing the necessity of restrictions[95], but this is particularly limited in the case of interference in the freedom of the press and freedom of broadcasting (as partial manifestations of the fundamental right under Art. 10 ECHR).[96] This applies insofar as the respective media act with the aim of informing the public about socially relevant topics[97], thus fulfilling the task of a public watchdog[98]. It also applies outside the area of the "professional press" in the sense of an alignment of the scope of protection to situations typically threatening fundamental rights, provided that non-journalistic persons and lay journalists are in a situation comparable to that of the press with regard to their publication activities.[99] Publicly accessible media archives

92 ECtHR, judgement of 8.11.2012, no. 43481/09.
93 Cf. on hate speech for example ECtHR, judgement of 9.2.2012, no. 1813/07; of 16.7.2009, no. 15615/07.
94 ECtHR, in: EuGRZ 1995, p. 20.
95 *Daiber*, in: Meyer-Ladewig/Nettesheim/von Raumer, Art. 10 para. 33 with further references.
96 Cf. on this ECtHR, judgements of 7.6.2012, no. 38433/09; of 10.5.2011, no. 48009/08.
97 ECtHR, judgement of 6.1.2015, no. 70287/11; of 17.7.2001, no. 39288/98: "The Court considers that these principles also apply to the publication of books in general or written texts other than the periodical press".
98 ECtHR, judgement of 20.5.1999, no. 21980/93.
99 On the question whether a differentiation between classical journalists and other publicists within the personal scope of protection is compatible with Art. 10 ECHR, cf. ECtHR, judgement of 4.11.2014, no. 30162/10.

also play an increasingly important role in this context.[100] The particular relevance of the media to the formation of public opinion and their importance for a functioning democracy not only comes to bear within the framework of limited national margins of appreciation but also within the framework of the consideration to be carried out in the event of infringements of the fundamental rights of third parties.

In addition to issues of the protection of minors and of public safety and order, especially in the area of criminal law content, this applies above all to the impairment of the right to privacy (Art. 8 ECHR) of persons affected by a report or portrayed in media content. Due to the diversity of possible causes, a differentiated case law of the ECHR has developed over the years, from which numerous factors can be derived that play a role in the weighting of conflicting rights.[101] These include factors such as contributing to a debate of general interest, the role, function and past public behaviour of the person concerned, the nature of the activity being reported on, the way information is obtained, the truth of the content, and its form and impact. At least similar criteria are used by the ECtHR in conflicts with other rights of third parties, which may have a different direction of protection than the general right to privacy. This applies in particular to collisions between freedom of the media and copyright law, which, according to the ECtHR, are not fully protected even at the level of the ECHR.[102] Intellectual property may be restricted where freedom of expression, as an essential basis of a democratic society, requires it in the context of a debate of public interest. Human dignity, however, is not open to balancing of conflicting rights.[103]

The central provision of guarantees under media law, and thus of relevance in connection with the regulation of (online) content at Union level, is Art. 11 para. 1 CFR which states that every person has the right to freedom of expression, including the freedom to receive and pass on information and ideas without interference by public authorities and regardless of national borders. Art. 11 para. 2 CFR also stipulates that freedom and pluralism of the media shall be respected. Here too, the term "media" covers traditional media such as the press, radio and films as well as any other

100 ECtHR, judgement of 19.10.2017, no. 71233/13.

101 Cf. on this and the following instead of many: ECtHR, judgement of 7.2.2012, no. 39954/08.

102 ECtHR, judgement of 10.1.2013, no. 36769/08.

103 See, however, on tendencies of weighing human dignity against other rights in the case law of the CJEU: *Schwarzburg*, Die Menschenwürde im Recht der Europäischen Union, pp. 267 et seq.

form of mass communication that already exists or will only emerge in the future, provided that it is addressed to the general public.[104] Art. 11 CFR has been conceived in close accordance with or, as far as the scope of protection is concerned, in direct adoption of Art. 10 ECHR. Only the limitation rule of Art. 10 para. 2 ECHR has not been adopted, because the CFR as a whole contains a horizontally applicable standard limitation rule in Art. 52 para. 1 CFR.[105] In contrast to the ECHR, Art. 11 CFR explicitly mentions freedom of the media and its plurality, whereby the special importance of the media for freedom of expression is expressed on the one hand, but freedom of the media is also emphasised on the other hand from the context of a uniform fundamental right to communication.[106] In contrast to a comprehensive and differentiated case law of the ECtHR, the case law of the CJEU is less pronounced with regard to freedom of communication. This is also due to the fact that traditional restrictions to the freedom of communication tend to fall within the sphere of responsibility of the Member States in view of the EU's limited powers.[107] However, the case-law of the ECtHR on Art. 10 ECHR can be relied on to a large extent here, which also results from the corresponding explanations of the preamble to Art. 11 CFR.[108] This applies at least to Art. 11 CFR in its form as a right of defence. The CJEU makes increasing use of the possible recourse to the principles of the ECHR and their development by the ECtHR and refers in its rulings to the corresponding relevant case-law including the limitations contained therein.[109]

2.1.2.5. Freedom to Conduct a Business

Freedom to conduct a business is enshrined in Art. 15 CFR in the section on civil liberties. The ECHR, on the other hand, does not contain an inde-

104 *Von Coelln*, in: Stern/Sachs, Art. 11 para. 30.
105 *Löffler*, Presserecht, § 1 para. 88; *Von Coelln*, in: Stern/Sachs, Art. 11 para. 7 et seq.
106 *Löffler*, Presserecht, § 1 para. 89, 90 with further references also to the debate as to whether Art. 11 para. 2 CFR is to be accorded a legally independent meaning by highlighting the wording of this provision.
107 *Löffler*, Presserecht, § 1 para. 46, 86.
108 Explanations relating to the Charter of Fundamental Rights, OJ C 303/17, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007X1214(01)&from=DE.
109 Cf. already CJEU, *Familiapress v Heinrich Bauer Verlag*, supra (fn. 38).

pendent regulation on freedom to conduct a business. However, partial elements of this freedom are also protected in the ECHR via individual fundamental rights. For example, freedom of expression from Art. 10 ECHR, the right to a fair trial from Art. 6 ECHR, freedom of property from Art. 1 of the First Additional Protocol to the ECHR and the right to respect for private life from Art. 8 ECHR are to be mentioned in this regard.[110]

Art. 15 CFR states that everyone has the right to engage in work and to pursue a freely chosen or accepted occupation; it states also that every citizen of the Union has the freedom to seek employment, to work, to exercise the right of establishment and to provide services in any Member State. However, this is not to be understood as a subjective position in the sense of a right to the creation of a – as appropriate as possible – job. According to the systematic position in Part 2 of the CFR, it is a purely fundamental right of freedom, which prohibits the Member States and the EU in principle from taking active steps to prevent people from taking up employment and thus from choosing and exercising a profession.[111] In the case law of the CJEU, however, there is no precise definition of the term "business". From a generous assumption on numerous gainful activities under the freedoms of the internal market, which is to be determined in the case law of the CJEU and the courts of the Member States, it can be concluded, however, that the freedom to conduct a business under Art. 15 para. 1 CFR is to be understood in a comprehensive sense.[112] Consequently, any economic activity, i.e. remunerated activity serving the purpose of acquisition, is also to be considered as a profession within the meaning of Art. 15 CFR if it is neither purely temporary nor absolutely minor in nature, whereby economic success is irrelevant in this respect.[113]

According to the case law of the CJEU, however, freedom to conduct a business does not apply in all its forms "without limits"; rather, it must be viewed in terms of its social function.[114] An encroachment on the freedom to conduct a business that requires justification is present in every sovereign act which has a perceptible negative effect on the choice or exercise of an occupation. With regard to the dissemination of online content and the corresponding enforcement of rights, online platforms and other service providers, in particular, may be severely restricted in their rights.

110 *Blanke*, in: *Stern/Sachs*, Art. 15, para. 14.
111 *Blanke*, in: *Stern/Sachs*, Art. 15, para. 24 et seq.
112 *Blanke*, in: *Stern/Sachs*, Art. 15, para. 28.
113 *Penski/Elsner*, in: DÖV 7/2001, p. 265, 271.
114 *Blanke*, in: Stern/Sachs, Art. 15, para. 43.

The business model of many providers is aimed precisely at being able to offer a large number of contents to a large audience without prior verification. Regulations that impose obligations on the platforms in this respect and, if necessary, provide for liability in the event of non-compliance thus constitute interference with their freedom of occupation.

The justification for such an intervention is based on Art. 52 para. 1 CFR. According to this, each interference must be based on a legal basis issued by the competent legislator. In addition, each infringement must comply with the principle of proportionality, therefore pursue a legitimate objective, be necessary and appropriate and must not affect the essence of the fundamental right.[115] Furthermore, it can be stated that Art. 15 CFR, with regard to the unity of the CFR, finds a direct barrier in other legal values guaranteed by the CFR.[116] Thus, a service provider can only exercise its freedom from Art. 15 CFR to such an extent that the fundamental rights of other rights holders whose contents are disseminated, for example, via platforms in the online area are also sufficiently taken into account. For example, the right to intellectual property contained in Art. 17 para. 2 CFR, which includes copyright, publishing, patent and trademark rights, or the right of a company to dispose of the information concerning its systems and products, should be mentioned here.[117]

2.1.2.6. Right to Property

The right to property is guaranteed in Art. 17 CFR and in Art. 1 of Protocol No. 1 to the ECHR (P1ECHR).

According to Art. 17 para. 1 CFR, everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. The term "possessions", i.e. the material scope of protection of the right to property, thus encompasses all monetary asset positions, i.e. in addition to the ownership of movable and immovable property, all acquired property rights which are exclusively assigned to a person by the legal system, provided that these have arisen by virtue of his own performance or at any rate from the assets of a natural or legal person.[118] Moreover, Art. 17 para. 2 CFR states that also intellectual property shall be protected. Corresponding to

115 *Blanke*, in: Stern/Sachs, Art. 15, para. 44.
116 *Blanke*, in: Stern/Sachs, Art. 15, para. 44.
117 *Vosgerau*, in: Stern/Sachs, Art. 17, para. 44.
118 *Vosgerau*, in: Stern/Sachs, Art. 17, para. 43.

Art. 17 para. 1 CFR, Art. 1 para. 1 P1ECHR states that every natural or legal person is entitled to the peaceful enjoyment of his possessions. However, the ECHR not only protects within the framework of this wording the ownership of property but in principle also includes certain rights and interests which constitute an asset and can, therefore, be equated with (tangible) property.[119] This also includes, although not explicitly mentioned here as in the CFR, intellectual property rights (copyright, trademark and patent rights), because these are rights which are assigned to the individual as exclusive rights and which she or he can generally freely dispose of.[120]

In the context of the cross-border dissemination of online content, different actors have to be considered in light of the right to property. On the one hand, the rights of those whose content is distributed via online platforms are significantly affected. The intellectual property just mentioned will often be affected here, whether in the sense of an original copyright or a license, which also has an asset value in the sense of the definition mentioned above. On the other hand, however, platforms are also affected which first make the content available to an audience. Regulations that impose obligations or restrictions on platforms or other distributors can interfere with the basic right to property of the platform provider. Although the CJEU has already frequently dealt with the protection of the property of companies and in principle also subjects companies to the right to property, it has not explicitly recognised, so far, a right to the established and exercised business which goes beyond the individual operating resources already covered by the property right and would aim at the company as a whole.[121] However, according to the case law of the ECHR, economic interests affecting the running of a business are also considered to be within the scope of protection of the right to property. According to the CFR, these "soft factors" should in any case also participate in the protection of property when the existence of the (ownership protected) company itself is at stake. Due to extensive obligations imposed on platform operators with regard to the distribution of online content, the business model of various providers can be severely endangered and is thus a position capable of protection in the sense of this fundamental right.

---

119 *Meyer-Ladewig/von Raumer*, in: Meyer-Ladewig/Nettesheim/von Raumer, Art. 1 Protocol No. 1 to the ECHR, para. 11.

120 On the character of intellectual property rights as property in the sense of Art. 1 P1ECHR cf. already *Peukert*, EuGRZ 1981, p. 97; *Vosgerau*, in: Stern/Sachs, Art. 17 para. 44.

121 *Vosgerau*, in: Stern/Sachs, Art. 17, para. 35.

In this context, the enforcement of rights by means of instruments provided for this purpose by the legal system can mean an interference in the legal position of another legal subject. An interference of the right to property is given if either an ownership position is withdrawn or its use, disposal, inheritance or exploitation is subject to restrictions. In this respect, the CJEU, in its previous case-law, has essentially adopted the concept of ownership interference from the ECHR. An intervention may, however, be justified under the requirements provided for this purpose. When examining the justification, a distinction must be made between the withdrawal of ownership and restrictions on its use based on the wording of Art. 17 CFR (and also Art. 1 P1ECHR). For the distribution of online content, the restriction of the use of proprietary protective positions is decisive. A mere restriction on the use of property is justified if it serves objectives which are in the public interest of the Union, if it does not present itself as unacceptable, i.e. excessive, with regard to the purpose pursued and if it therefore does not affect the substance of the property right.

2.1.3. Fundamental Rights Protection Obligations

With regard to the ECHR, the fundamental existence of obligations to protect ("positive obligations" or "*obligations positives*") – derived from duties to act – can be established by interpreting a series of judgments of the ECtHR.[122] At the same time, however, on the basis of the ECHR there is a scope for implementation by the states in the exercise of their protection obligations, so that the protection obligation does not necessarily have to be followed by a statutory regulation; instead, investigation obligations and information obligations can also be considered.[123]

The ECtHR has, for example, recognised such "positive obligations" for Art. 8 ECHR[124] and Art. 10 ECHR. With regard to the former, obligations of the contracting states may result from human rights, particularly in the

122 Cf. ECtHR, judgement of 16.3.2000, no. 23144/93, para. 42; *Dröge*, Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, pp. 1 et seq., 71 et seq., 179 et seq.; *Jaeckel*, Schutzpflichten im deutschen und europäischen Recht, pp. 128 et seq.; *Klatt*, in: ZaöRV 71, 2011, p. 691, 692 et seq.; *Koenen*, Wirtschaft und Menschenrechte, p. 58; *Ress*, in: ZaöRV 64, 2004, p. 621, 628.

123 Cf. *Koenen*, Wirtschaft und Menschenrechte, p. 59 et seq.

124 ECtHR, judgement of 27.10.1994, no. 18535/91, para. 31; judgement of 12.11.2013, no. 5786/08, para. 78.

area of the right to sexual self-determination, respect for good reputation, the right to one's own image and the protection of personal data. With regard to the freedom of the media, the contracting parties must effectively guarantee pluralism, particularly in the audiovisual media, through an appropriate framework.[125] Freedom of expression can also trigger such obligations.[126] Furthermore, the ECtHR assumes positive obligations under Art. 2, 3, 6 and 11 ECHR[127], whereby such positive obligations to act can also be considered for other rights. In a decision concerning Art. 10 ECHR, the ECtHR explained the criteria for the assumption of a positive duty to protect:

> "In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual, the search for which is inherent throughout the Convention. The scope of this obligation will inevitably vary, having regard to the diversity of situations obtaining in Contracting States, the difficulties involved in policing modern societies and the choices which must be made in terms of priorities and resources. Nor must such an obligation be interpreted in such a way as to impose an impossible or disproportionate burden on the authorities"[128].

This shows that a weighing up of fundamental rights at the level of justification, which is regularly required in the framework of fundamental rights, can already play a role in the assessment of the warranty content of fundamental rights. The more an existing grievance interferes with fundamental rights, the more government action will be necessary.

With regard to human dignity – as an inviolable good and as the highest principle which also affects other human rights – and its relevance in the area of online content (cf. Chapter 2.1.2.1), one will be able to ascertain serious grievances concerning human dignity in the digital environment, especially if one includes the *dark web*. With regard to Art. 3 ECHR, the ECtHR already ruled on the emergence and scope of state protection obligations which, however, directly only concern the actual (physic or psy-

125 ECtHR, judgement of 22.4.2013, no. 48876/08 para. 134; judgement of 17.9.2009, no. 13936/02 para. 100 et seq.
126 ECtHR, judgement of 29.02.2000, no. 39293/98; judgement of 16.03.2000, no. 23144/93.
127 For an overview see ECtHR, judgement of 16.3.2000, no. 23144/93, para. 42.
128 ECtHR, judgement of 16.3.2000, no. 23144/93, para. 43.

chic) threat or existence of inhuman or degrading acts and not their depiction or making available on the Internet. Accordingly, protective measures are necessary if state authorities know or must know of such a danger, which applies in particular and to a special extent to the danger of child abuse.[129] In this case, they must intervene effectively and with due regard to the interests of the victims, which also implies legislative measures.[130] Although the (psychological) burden of depicting acts violating human dignity in the context of online content and the resulting (renewed) impairment of human dignity may not be comparable with the actual (psychological and physical) burden of the depicted act, there is at least a connection and a similarity. Against this background, it seems contradictory to impose protective duties on the state, for example, if torture is committed against a person, but not if a video of this act of torture is published on the Internet. As shown above, both can affect human dignity, albeit in different ways.

With regard to the question of positive protection obligations of the Member States under the CFR, two things should first be mentioned: On the one hand, such obligations can only be imposed on Union law bodies if they have original Union law competence in this area and if their action in accordance with the principle of subsidiarity is precisely required, and the Member States can only be imposed if they implement Union law. Another approach would conflict with Art. 51 para. 2 CFR, according to which the CFR does not extend the scope of Union law beyond the competences of the Union and has no influence on existing competences.[131] On the other hand, Art. 51 para. 1 sentence 2 CFR states an obligation for the Member States to promote, but it should not in principle be interpreted in such a way that positive legal protection obligations of the Member States result from the fundamental rights in general. Rather, in principle, each individual fundamental right of the Union must be examined with regard to its content under the law of compulsory protection.[132] If such state protection obligations exist at Union level, there is much to suggest that these can also include warranty obligations in the organisation and design of procedures as well as information obligations.[133]

---

129 ECtHR, judgement of 28.10.1998, no. 23452/94, para. 116 et seq.
130 ECtHR, judgement of 22.3.2016, no. 646/10, para. 72 et seq.
131 Cf. Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, pp. 17–35.
132 *Ladenburger/Vondung*, in: Stern/Sachs, Art. 51 para. 21 et seq.
133 *Weber*, in: Stern/Sachs, Art. 7 para. 5 with further references.

The CJEU has so far been rather cautious in its explicit acceptance of state protection obligations under the fundamental rights of the Charter. It has indicated such obligation, for example, for the right to property[134]; the CJEU has, however, in particular with regard to intellectual property, tended to focus on secondary legislation dealing with the right to property and has not dealt with the question of positive protection obligations (despite its possibility to deal with).[135] The same applies to the protection of private life under Art. 7 CFR against the background of secondary data protection law.[136] With regard to the rights of the child, for example, which are guaranteed in Art. 24 CFR, Art. 14 and Art. 24 para. 2 CFR provide for the participation of the state in the upbringing of children and thus also in the concretisation of the best interests of the child, whereby Art. 24 para. 3 indicates that this guardian function is the responsibility of the Member States and not of the Union itself.[137] Thus, the fundamental duties of protection in favour of the best interests of the child are stipulated here, the concrete contents of which, however, have to be determined by the national legislature.[138]

Due to the relationship between ECHR and CFR described at the beginning of this section, but also due to the CJEU's reference to the principles developed by ECtHR in the framework of its case law on fundamental rights of the Union, it will, however, also be possible to transfer the ECtHR's doctrine of the duty to protect to Union level, provided that this does not contradict the special characteristics described in Art. 51 and, in particular, that there remains a margin for manoeuvre for the Member States.

134 CJEU, judgement of 24.3.1994, C-2/92, *The Queen v Ministry of Agriculture, Fisheries and Food, ex parte Dennis Clifford Bostock*, para. 18 et seq.

135 Cf., e.g., CJEU, judgement of 29.1.2008, C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*.

136 Cf. on this CJEU, judgement of 8.4.2014, joint cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.

137 *Ennuschat*, in: Stern/Sachs, Art. 24 para. 12.

138 Cf. *Grabenwarter*, in: DVBl. 2001, p. 1, 6.

2.2. Fundamental Freedoms

2.2.1. Freedom of Establishment and Freedom to Provide Services

Freedom of establishment (Art. 49 et seq. of the Treaty of the Functioning of the European Union, TFEU[139]) includes the right to take up and pursue self-employment in another Member State in accordance with the provisions laid down by the latter for its own nationals, as well as the right to set up and manage businesses. The applicability of the material scope of protection requires the existence of an economic activity with cross-border implications. Both characteristics must be interpreted broadly.[140] With regard to the cross-border dissemination of online content, a profit-making purpose will usually be necessary. It can be assumed that this is normally the case, at least on the part of the disseminator of content. The notion of "establishment" implies a certain stability and durability and thus distinguishes the freedom of establishment from the freedom to provide services (Art. 56 et seq. TFEU). In the case of the former, it is important that the entrepreneur participates permanently in the economic market of another Member State by establishing a presence. By contrast, in the latter case, the provision of a cross-border service is of primary importance. The TFEU does not define durability any further. The CJEU has laid down various criteria, such as period and frequency, residential situation of the service provider or place of payment.[141] However, the notion of establishment has been refined in the area of media law, which is of particular relevance here. Art. 2 of the AVMSD contains a list of indicative facts according to which the place of establishment of a media service provider can be determined (and therefore which Member State is responsible for its regulation). The following facts are of particular relevance: the location of the head office and the place where editorial decisions are made or where a significant proportion of the staff responsible for the programming is based. Although these requirements only apply directly within the framework of the AVMSD, they can also be used for assessment purposes within the framework of freedom of establishment for media service providers.

---

139 Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47390. Provisions of the TFEU relevant in the context of this study are listed in the Online Annex, available at www.nomos-shop.de/44382, I.

140 *Korte*, in: Calliess/Ruffert, Art. 49 TFEU para. 12, 19 et seq.

141 *Korte*, in: Calliess/Ruffert, Art. 49 TFEU para. 26.

The players potentially involved in the dissemination of online content – broadcasters, on-demand providers, VSPs, intermediaries, search engines, apps, access providers, etc. – are heterogeneous. Thus they cannot be categorised as falling under the protective scope of the freedom of establishment per se. Rather, the protections offered by the freedom to provide services (Art. 56 et seq. TFEU) will more regularly apply for these actors, especially if they are information society services within the meaning of the ECD[142]. The freedom to provide services does not require a permanent change of seat nor integration into a legal system and thus corresponds more readily to the spontaneous cross-border (factor) mobility of online activity.[143] According to Art. 57 TFEU, services shall be considered to be "services" within the meaning of the Treaties where they are normally provided for remuneration, insofar as they are not governed by the provisions relating to freedom of movement for goods, capital and persons. However, in addition to this negative definition, which relies on a distinction from other fundamental freedoms, participation in commercial transactions by self-employed persons is regularly taken into account.[144] In its case-law, the CJEU has characterised the crossing of borders and remuneration as indispensable characteristics of a service. The notion of service must be interpreted broadly and can already be assumed to exist if the activities constitute part of economic life.[145] This includes "cultural activities" such as radio and television[146] as well as gambling[147]. It (usually) does not matter who pays the fee, whether it is the customer/user or a third party such as an advertising partner. This is particularly relevant for advertising-financed offers such as private broadcasting, for the countless offers on the Internet that are financed via advertising business models such as VSPs or for social networks like Facebook or adult content platforms.

142 Cf. on this recently the Opinion of Advocate General Szpunar delivered on 30.4.2019, C-390/18, *AirBnB*, para. 19 et seq.
143 *Kluth*, in: Calliess/Ruffert, Art. 56 TFEU, para. 1.
144 *Randelzhofer/Forsthoff*, in: Grabitz/Hilf/Nettesheim, Art. 49, 50 TFEU, para. 80.
145 CJEU, judgement of 12.12.1974, C-36/74, *B.N.O. Walrave and L.J.N. Koch v Association Union cycliste internationale, Koninklijke Nederlandsche Wielren Unie and Federación Española Ciclismo*, para. 4; of 5.10.1988, C-196/87, *Udo Steymann v Staatssecretaris van Justitie*, para. 9.
146 Fundamentally: CJEU, judgement of 30.4.1974, C-155/73, *Giuseppe Sacchi*.
147 CJEU, judgement of 22.3.1994, C-275/92, *Her Majesty's Customs and Excise v Gerhart Schindler and Jörg Schindler*; judgement of 6.11.2003, C-243/01, *Criminal proceedings against Piergiorgio Gambelli and Others*.

It has not yet been expressly clarified by the CJEU whether payment with user data, for example in return for the use of a free digital service, is to be regarded as payment in this sense. As a result of new efforts at EU level, in particular by the Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services[148], which recognises data as quasi-contractual consideration in the case of digital services[149], an interpretation in this sense is very likely.[150] However, such offers will regularly rely, at least partially, on advertising finance, which is enhanced by the collection, analysis and use of user data in the context of, for example, personalised advertising.[151]

However, either the freedom of establishment or the freedom to provide services will regularly be affected. It follows from the case law of the CJEU that an economic activity – which regularly exists in the online activities considered here – falls under either the freedom of establishment or the freedom to provide services.[152] The provisions on services are complementary to those on the right of establishment: the wording of Art. 56 para. 1 TFEU already requires that the provider and recipient of the service in question are "established" in two different Member States. Art. 57 TFEU stipulates that the provisions on services apply only if the provisions on the

148 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136, 22.5.2019, pp. 1–27. According to Recital 36 of this directive, however, this directive should (expressively) be without prejudice to other Union law governing a specific sector or subject matter, such as telecommunications, e-commerce and consumer protection. It should also be without prejudice to Union and national law on copyright and related rights, including the portability of online content services.

149 Art. 3 para. 1 of Directive (EU) 2019/770 states: "This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader […]."

150 Cf. on this Directive also *Schmidt-Kessel/Erler/Grimm/Kramme*, in: ZPEU 13(1), 2016, p. 2; and *Bokor*, Die Richtlinienvorschläge der Kommission zu Verträgen über digitalen Inhalt und Online-Warenhandel, available at https://www.bundestag.de/resource/blob/422554/6f0bd347b413226ad2ffe992dc5cfa9f/bokor-data.pdf.

151 Cf. on data driven business models *Seufert* (ed.), Media Economics revisited: (Wie) Verändert das Internet die Ökonomie der Medien?, pp. 38 et seq.

152 CJEU, judgement of 30.11.1995, C-55/94, *Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano*, para. 2.

right of establishment are not applicable.[153] When examining whether exemptions to the freedom of establishment or the freedom to provide services are justified, it is not necessary to make a separate assessment for each freedom when looking at the context of the online dissemination of the relevant content. The requirements for justifying exemptions to the two fundamental freedoms do not differ significantly from each other. In the following, solely the effects of the freedom to provide services in the area of online content dissemination will be discussed.

The freedom to provide services contains a prohibition of discrimination and a prohibition of restrictions.[154] In addition to the active freedom to provide services, i.e. the freedom of the service provider to provide his service in another Member State under the same conditions as a service provider established there, it also protects the passive freedom to provide services[155], i.e. the recipient's right to receive a service in another Member State from a service provider established there.

In this context it has often been discussed whether – and if so, to what extent – the freedom to provide services requires the implementation of the country-of-origin principle.[156] According to the CJEU, a provision is already restrictive and thus a limitation of the freedom to provide services if it requires an additional administrative or economic effort on the part of the service provider. This is meant to protect the service provider from a double burden (obligations under the laws of the country of origin and the country of destination).[157] The country-of-origin principle, on which, inter alia, the AVMSD and the ECD are based, avoids such double burdens (in principle), since it binds the service provider (in principle) only to the obligations provided in his country of origin. Art. 56 et seq. TFEU are primari-

153 Ibid., para. 22; Cf. also judgements of 12.12.1996, C-3/95, *Reisebüro Broede v Gerd Sandker*, para. 19; judgement of 11.3.2010, C-384/08, *Attanasio Group Srl gegen Comune di Carbognano*, para. 39.

154 Established jurisprudence since CJEU, judgement of 3.12.1974, C-33/74, *Johannes Henricus Maria van Binsbergen v Bestuur van de Bedrijfsvereniging voor de Metaalnijverheid*; for the freedom of establishment in parallel, cf. *Korte*, in: Calliess/Ruffert, Art. 49 TFEU para. 49.

155 Cf. on this *Randelzhofer/Forthoff*, in: Grabitz/Hilf/Nettesheim, Art. 49/50 TFEU para. 51.

156 Cf. on this in detail *Waldheim*, Dienstleistungsfreiheit und Herkunftslandprinzip; *Albath/Giesel*, in: EuZW 2, 2006, p. 38, 39 et seq.; *Hörnle*, in: International and Comparative Law Quarterly 54(1), 2005, p. 89.

157 CJEU, judgement of 15.3.2001, C-165/98, *Criminal proceedings against André Mazzoleni and Inter Surveillance Assistance SARL, as the party civilly liable, third parties: Eric Guillaume and Others*, para. 24.

ly intended to dismantle barriers to market access; however, they do not specify how equivalence is to be established for service providers. The CJEU derives from the freedom to provide services at least an obligation of the Member States to examine whether equivalence and recognition exists, i.e. whether control measures already carried out (equivalent and recognisable) in the country of origin may not be carried out again[158]. However, this does not mean that the legal situation of the country of origin takes precedence in principle. It merely obliges the Member State to take account of it. The freedom to provide services therefore does not necessarily require the application of the country-of-origin principle. This seems logical insofar as, on the one hand, the country-of-origin principle can also have a restrictive effect on the service provider, where for example the legal situation in the country of destination is more favourable. On the other hand, this is supported in particular in the interest of consumer protection, which prohibits that service providers be bound per se only by the law of their country of origin. This is meant to prevent situations whereby consumers would be subject to a legal uncertainty due to a lack of knowledge of the legal situation in the origin Member State and the service provider itself.[159]

Finally, it should also be noted that a restriction on the freedom to provide services needs to be justified. In addition to the justifications expressly provided for by the TFEU – public security, public order and public health – other restrictive measures may also be justified if they are necessary in order to pursue an objective in the public interest and if they are applied appropriately and do not go beyond what is necessary in order to achieve that objective (i.e. meet the proportionality test).[160] Exceptions to the country-of-origin principle and the scope of application of the country-of-destination principle must always be measured against these criteria, in particular when drafting national or European legislation.

For example, the objective of ensuring the quality of services or protecting customers from harm may be such an objective of general interest. The resulting obligations for undertakings, such as registration obligations, must not extend to the provision of occasional services and must not give

158 Cf. on this, e.g., CJEU, *Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano*, supra (fn 152).

159 *Kluth*, in: Calliess/Ruffert, Art. 56 TFEU para. 3 et seq.

160 CJEU, judgement of 13.1.1993, C-19/92, *Dieter Kraus v Land Baden-Württemberg*, para. 32; judgement of 26.10.1995, C-272/94, *Criminal proceedings against Michel Guiot and Climatec SA, as employer liable at civil law*, para. 11.

rise to additional administrative or contribution costs.[161] Other objectives of general interest recognised by the CJEU which are relevant in the context of this study are cultural policy[162], the protection of intellectual property[163], consumer protection[164] and the protection of minors[165]. Whether these objectives are pursued by appropriate and proportionate means is a matter for the individual case but depends in particular on the intensity of the restriction imposed.

2.2.2. Free Movement of Goods

The free movement of goods (Art. 28 et seq. TFEU) will only be briefly discussed in the present context, as it has only minor relevance for the cross-border dissemination of online content. It covers the free exchange of goods (movable physical items with a basic monetary value) within the Union and therefore protects against restrictions on the movement of goods. Online content is typically distributed in a digital format. The CJEU analyses the nature of a service by referring to the main activity of the service. For example, in the case of television broadcasts, the main activity is not the transmission but the production of content and thus subject to the rules on the freedom to provide services.[166] Although content can be fixed on physical media such as hard disks or the smartphone memories, in the context of online distribution this is normally only carried out by the user on an occasional basis. The online distribution of content is usually about consumption and not ownership. The freedom to provide services applies to non-physical products such as digital media content which is not distributed on a storage medium.

---

161 CJEU, judgement of 30.11.1999, C-58/98, *Josef Corsten*, para. 38 et seq.
162 CJEU, judgement of 25.7.1991, C-353/89, *Commission of the European Communities v Kingdom of the Netherlands*.
163 CJEU, judgement of 18.3.1980, C-62/79, *SA Compagnie générale pour la diffusion de la télévision, Coditel, and others v Ciné Vog Films and others*.
164 CJEU, judgement of 4.12.1986, C-220/83, *Commission of the European Communities v French Republic*.
165 CJEU, judgement of 8.9.2009, C-42/07, *Liga Portuguesa de Futebol Profissional and Bwin International Ltd v Departamento de Jogos da Santa Casa da Misericórdia de Lisboa*.
166 CJEU, *Sacchi*, supra (fn. 146).

2.3. Other Elements of EU Primary Law

2.3.1. Fundamental Principles and Goals of the EU

The Treaty on European Union (TEU)[167] is, alongside the TFEU, the basis for the European Union. It lays down its constituent structural principles and thus defines its essential legitimating foundations. All regulatory measures of the EU and its Member States must therefore always be viewed in the light of the TEU: they must meet its requirements and take its fundamental values into account. Art. 2 and 3 of the TEU elaborate the basic values and objectives of the EU. They are of particular importance.

Art. 2 TEU establishes the foundational values of the Union: respect of human dignity, freedom, democracy, equality, the rule of law and respect of human rights, including the rights of minorities. The respect of human rights not only substantiates human dignity and the principle of freedom but also the rule of law within the EU.[168] It thus builds a bridge to the fundamental rights addressed in the first section of this chapter.

These values are common to all Member States, i.e. in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail. Even though Art. 2 TEU is therefore primarily aimed at the EU itself, as can be seen from sentence 2, these fundamental values also have significance under Union law with regard to the legal systems of the Member States. Thus, on the one hand, the aforementioned fundamental values acquire significance as a substantive prerequisite in the accession procedure under Art. 49 TEU. On the other hand, their non-compliance in the procedure under Art. 7 TEU can lead to a restriction or suspension of Member State rights, including voting rights.[169] In addition to the fundamental requirement of Member States to remain loyal to the Union, derived from Art. 4 para. 3 subpara. 2, this is a further,

167 Treaty on European Union (TEU), OJ C 326, 26.10.2012, pp. 13–390. Provisions of the TEU relevant in the context of this study are listed in the Online Annex, available at www.nomos-shop.de/44382, I.

168 *Calliess*, in: Calliess/Ruffert, Art. 2 TEU para. 27.

169 This procedure is currently of importance for the first time with regard to the Member States Poland and Hungary, whereby the (political) discussion also refers to restrictions on freedom of the media and diversity of opinion in these Member States. Cf. *Ukrow*, in: vorgänge No. 224, 4/2018, p. 57, 62. Cf. also the Opinion of Advocate General Sharpston, delivered on 31.10.2019, C-715/17, C-718/17 and C-719/17 in the proceedings against Poland, Hungary and the Czech Republic.

more concrete mechanism for coordinating measures within the EU along the lines of adherence to fundamental values.

Art. 3 TEU sets out the objectives to be achieved through integration of the Union. These objectives are meant to provide a goal-oriented framework for action and ensure that integration is not just pursued for its own sake.[170] The provision therefore lays down a final EU programme, which must be achieved by EU institutions with respect to the latter's limited competencies and in the relevant thematic and legal areas through coordinated policy action by Member States. This can also result in standstill obligations for the Member States, which may prohibit them from counteracting the integration targets set by the EU.[171] According to Art. 4 para. 3 subpara. 3 TEU, the Member States shall instead assist the Union in carrying out its task and shall refrain from any measure which could jeopardise the attainment of the objectives of the Union.

Art. 3 TEU lists several objectives which are also relevant in the context of this study. According to Art. 3 para. 2 TEU, the Union shall, among other things, establish an internal market, work towards the sustainable development of Europe on the basis of balanced economic growth and a highly competitive social market economy, and promote scientific and technical progress. With regard to the distribution of online content and the digital economy as a whole, the strategy for a digital single market for Europe as a manifestation of these objectives is particularly important.[172] The Commission considers that the Digital Single Market should provide better access to digital goods and services, create an optimal environment for digital networks and services, and ensure that Europe's economy benefits from the digital revolution as a growth engine. Distributors/providers of online content are therefore meant to benefit as a priority from a (better) economic and regulatory environment that is to be created as part of this strategy. The EU has already tackled some reform projects under the umbrella of the Digital Single Market strategy. These include in particular the promotion of electronic commerce by abolishing geo-blocking, the modernisation of EU copyright law to adapt to the digital age and the updating of

170 *Ruffert*, in: Calliess/Ruffert, Art. 3 TEU para. 3; in principle regarding the objectives cf. *Müller-Graf*, in: Pechstein/Nowak/Häde, Art. 3 TEU para. 1; *Heintschel von Heinegg*, in: Vedder/Heintschel von Heinegg, Art. 3 TEU para. 3.

171 *Ruffert*, in: Calliess/Ruffert, Art. 3 EUV para. 4, 7.

172 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

EU rules on audiovisual content, implemented through the adoption of the Geo-blocking Regulation[173], the new DSM Directive and the reformed AVMSD. Meanwhile, other reform projects, such as the adaptation of the rules on privacy in electronic communications to the new digital environment, are still pending.[174] A closer look at the reforms that have already taken place shows, however, that not only the interests of the digital economy have been taken into account but that the interests of other stakeholders, in particular consumers, have played a central role, too. For example, combating illegal online content and protecting the most vulnerable users has been a key concern of the AVMSD reform, reflected for example in new rules for video-sharing platforms.

This in turn corresponds to a further objective of Art. 3 para. 3 subpara. 2 TEU, according to which the Union fights social exclusion and discrimination and promotes social justice and the protection of the rights of children.

Finally, Art. 3 para. 3 subpara. 4 TEU plays a role in the context of media policy as a whole and therefore in the context of this study. According to this, the EU shall respect its rich cultural and linguistic diversity and shall ensure that Europe's cultural heritage is safeguarded and enhanced. This provision therefore addresses the role of media as economic and cultural heritage in safeguarding diversity. Thereby the EU's objective is not to create a uniform European culture but rather to preserve existing cultural diversity, which draws its strengths precisely from its historically grown diversity. Against this background, measures at national level which are necessary for the protection of national and regional languages and cultures

173 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 60I, 2.3.2018, pp. 1–15.

174 Cf. on this the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD), which, according to the Commission's original objective, was to enter into force at the same time as the GDPR but is still in the trilogue procedure.

are advocated at European level, as they ultimately make a contribution to cultural diversity – one of Europe's fundamental values.[175]

In the context of this study, Art. 2 and 3 TEU therefore mean two things: Firstly, the Member States must comply with the basic values established by the EU and meet the targets set. Different basic values and targets must be reconciled. Secondly, this gives rise to a responsibility on the part of the EU: On the one hand, where standstill obligations for the Member States exist, resulting from Art. 3 in conjunction with Art. 4 para. 3 TEU, the Union must – where it is assigned a competence – at least react to existing grievances which endanger the objectives. On the other hand, it should also be mentioned that no direct concrete duties to act can be derived from Art. 2 and 3 TEU.

2.3.2. Relevant EU Competencies

2.3.2.1. Legal Bases for an EU Competence in the Media Sector

However, the establishment of goals in accordance with Art. 3 TEU does not result in an allocation of powers. The EU can therefore only act within the framework of its competence to implement these goals.[176] All competences not conferred on the Union by the Treaties remain with the Member States in accordance with Art. 5 TEU, which addresses the principle of limited power, whereby the Union acts only within the limits of the powers conferred on it by the Member States in the Treaties to attain the objectives set out therein. These are exclusive competences (Art. 3 TFEU), shared competences (Art. 4 TFEU) or competences to support, coordinate or supplement the actions of the Member States (Art. 6 TFEU). The nature of each competence also determines the respective powers to act of both the Union and the Member States.

Exclusive competences, under which, in principle[177], only the EU can take legislative actions, exist in particular for "the establishing of the competition rules necessary for the functioning of the internal market". Art. 101 et seq. TFEU are expressions of the exercise of this competency. They also form the core of EU competition policy, which contains provi-

175 Cf. further *Ukrow/Cole*, Aktive Sicherung lokaler und regionaler Medienvielfalt, pp. 56 et seq.
176 *Ruffert*, in: Calliess/Ruffert, Art. 3 TEU para. 37.
177 However, the EU can continue to empower Member States to act.

sions on prohibitions of cartels, abuse of market power and on combating state restrictions on competition in the form of monopolisation and state aid.

Although the functioning of the internal market is a prerequisite for a matter to be allocated exclusive EU competence, the internal market (Art. 114 TFEU) itself does not fall under the exclusive competence of the EU.[178] On the contrary, Art. 4 para. 2 TFEU – like consumer protection – defines it as a shared competence[179], under which both the Union and the Member States have the possibility of adopting legally binding acts, whereby the Member States can only take action to the extent that the Union has not taken action.[180]

Finally, under Art. 6 lit. c only support, coordination and complementary measures can be taken by the EU in the field of culture, which is therefore fundamentally and intrinsically the responsibility of the Member States. In principle, the EU is free to choose which instruments it uses for support and coordination, which may also include the enactment of binding legislation in the form of regulations or directives. However, it is limited to the extent that the basic power to regulate must remain with the Member States. Harmonisation of national legislation is therefore excluded.[181]

For the cultural sector this means that Art. 167 para. 1–3 TFEU enable, and at the same time limit, the active cultural policy of the EU. Thus, the EU should contribute to the development of the cultures of the Member States and promote cooperation between them, supporting and supplementing their activities where necessary, amongst others in the field of artistic and literary creation, "including in the audiovisual sector". This is relevant insofar as the regulation and law enforcement concerning the dissemination of online content normally concerns the media – in the sense of a broad understanding of the term – or at least involves media indirectly. Within the framework of Art. 167 para. 1–3 TFEU, however, EU cultural policy is not intended to counteract, unify or replace the policy of the Member States. It is (merely) to play a role as a guardian of European cul-

178 *Frenz*, Handbuch Europarecht, para. 2217 with further references.
179 *Calliess*, in: EuzW 1995, p. 693, 694 et seq.; *Ludwigs*, in: EuZW 19(2004), p. 577.
180 *Calliess*, in: Calliess/Ruffert, Art. 2 AEUV para. 12 with reference to other views which assume that competence under Art. 4 is originally in the hands of the Member States and is only superseded by Union action.
181 *Calliess* in: Calliess/Ruffert, Art. 2 AEUV para. 28.

tural creation and otherwise act in an entirely subsidiary manner.[182] Art. 167 para. 4 TFEU, a "cross-cutting cultural clause", establishes a rule for EU action outside the areas of cultural policy referred to in para. 1–3. According to this, the Union shall take cultural aspects into account when acting under other provisions of the Treaties. This, however, does not affect the EU's basic competence order, for example in the sense of an "*exception culturelle*". Art. 167 para. 5 TFEU determines the instruments and procedures available to the EU. Only recommendations adopted by the Council on a proposal from the Commission, as well as support measures adopted by the European Parliament and the Council in accordance with the ordinary legislative procedure and after consulting the Committee of the Regions, but excluding any harmonisation of the laws and regulations of the Member States[183], can be considered. The latter negative clause prevents the EU from recourse to the general titles of competence under the approximation of laws, particularly in the area of the internal market (Art. 114 TFEU), and regards special provisions on the harmonisation of laws.[184] Thus, this provision does not present itself as a general prohibition of harmonisation for measures *with an impact* on the cultural sphere but rather as a prohibition of harmonising cultural measures.

It follows from this system in Art. 167 TFEU that the EU, based on a legal basis from its catalogue of competences, can also act (regulating) beyond the obligations under Art. 167 TFEU.[185] However, the prerequisite resulting from the cultural cross-cutting clause is that it must take cultural aspects into account, which regularly amounts to a balancing of cultural and other regulatory interests (e.g. economic aspects). Moreover, it follows from the TFEU system that cultural aspects must not be at the centre of a regulation under Union law.[186]

In the case of questions and problems relating to the cross-border dissemination of online content, it is not possible to define a specific, relevant

182 Cf. on this in detail and with further references *Ukrow/Cole*, Aktive Sicherung lokaler und regionaler Medienvielfalt, pp. 60 et seq.

183 The importance of this exclusion was also emphasised by the Court of the European Union in its judgment of 10 May 2016; cf. EC, judgement of 10.5.2016, T-529/13, para. 101 et seq., *Izsák and Dabis*.

184 *Blanke*, in: Calliess/Ruffert, Art. 167 para. 19; similar: *Niedobitek*, in: Streinz, Art. 167 TFEU, para. 55.

185 *Lenski*, Öffentliches Kulturrecht, p. 142.

186 Established jurisprudence of the CJEU, cf., e.g., CJEU, judgement of 17.3.1993, C-155/91, *Commission of the European Communities v Council of the European Communities*.

area of law. Rather, various matters are involved here, different objectives can be pursued with legislation, and even addressees and contents may not be uniform. Thus, substantive legal rules on lawfulness or liability play just as much a role as more formalistic legal questions of law enforcement and jurisdiction. Accordingly, the rules that are relevant in this context are spread out among a number of different sets of laws such as the AVMSD, the DSM Directive and the ECD, which interact with each other and cannot be considered separately. It is therefore not surprising that in the area of "media policy" and in view of the complex nature of media goods and services, which can be defined neither solely as cultural goods nor simply as economic goods, competences are based on various legal bases in the TFEU: namely Art. 28, 30, 34, 35 (free movement of goods), 45–62 (free movement of persons, services and capital), 101–109 (competition policy), 114 (technological harmonisation or the use of similar technological standards, for instance, in Internet productions), 165 (education), 166 (vocational training), 167 (culture), 173 (industry) and 207 (common commercial policy).[187]

2.3.2.2. The Specific Legal Bases for the ECD

At the time of its adoption the ECD was based mainly on Art. 47 para. 2 in conjunction with Art. 55 and 95 of the Treaty establishing the European Community[188], i.e. competences arising out of the completion of the internal market.

The legislative competence established by Art. 47 para. 2 and Art. 55 of the EC Treaty (now Art. 53 para. 1 and 62 TFEU) in the field of recognition of qualifications, taking up and pursuing self-employed activities and providing services falls under the area of shared competence under Art. 4 para. 2 lit. a TFEU. It allows the Union to recognise and coordinate national law in this area, in particular in the form of Directives[189] as the strongest

187 Cf., e.g., European Parliament, Fact Sheets on the European Union, 2019, http://www.europarl.europa.eu/ftu/pdf/en/FTU_3.6.2.pdf.

188 Treaty establishing the European Community, as amended by the Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ C 340, 10.11.1997, pp. 1–144.

189 The adoption of a regulation based solely on Art. 53, 62 TFEU would not be possible. Cf. on this *Korte*, in: GewArch 6(2013), p. 230, 232.

legislative instrument possible in this framework.[190] The aim of this competence is to help those wishing to set up or provide services with the expansion of their services from the origin Member State to other destinations within the EU. Legal harmonisation was meant to improve the exercise of cross-border activities, an objective which is also protected and advocated by the fundamental freedoms. The starting point for any coordinative action is therefore a legal provision in the Member States which contains substantive provisions on an economic activity covered by the freedom of establishment or the freedom to provide services. This may also concern the coordination of administrative procedures[191], but it must also comply with the other requirements of Art. 53 TFEU.

This area has been substantiated to an extensive degree by CJEU case law, which prohibits the use of these provisions as general competence under the objective to regulate the internal market.[192] The CJEU has required, for one, the identification of a (sufficiently probable) obstacle to free movement caused by diverging national legal provisions, and, secondly, the cessation of a positive internal market effect by the coordinative measure in the sense that it facilitates the exercise of the freedom of establishment or the freedom to provide services. The creation and functioning of the internal market must always be the focus and objective of the coordinative action, although the pursuit of other objectives, such as those based on special authorisation (even decisive ones[193]), remains possible, provided that this does not circumvent rules of competence which have not been allocated.

190 *Korte*, in: Calliess/Ruffert, Art. 53 para. 1.
191 *Korte*, in: Calliess/Ruffert, Art. 53 TFEU para. 11, with further references.
192 Cf. this and the following fundamentally: CJEU, judgement of 5.10.2000, C-376/98, *Federal Republic of Germany v European Parliament and Council of the European Union*.
193 Ibid., para. 3.

2.4. EU Secondary Law

This section looks at secondary legislation (already adopted and proposed) that plays a role in the field of regulation of online content. The diversity of content, dissemination channels and problems on the Internet is matched by the diversity of issues covered by the legislative acts.

The ECD is the main secondary legislation to be dealt with in the context of this study because of the horizontal approach it follows. It will therefore be dealt with in detail in the following (Chapter 3). In this chapter, only a first quick overview of the genesis of the Directive will be given.

The AVMSD will be presented extensively because it is the most recent revision of a content-related regulatory instrument of the EU, which from the outset of the ECD was regarded as being closely related (see, e.g., Recital 44 of the AVMSD). Especially due to the extension of the scope to VSPs it is relevant to study the Directive in more detail as it can be seen as an important step towards a more inclusive regulation of online service providers by the EU. While the ECD historical background relates to an Internet context which was completely different in terms of the important market players, the AVMSD reform was decided in light of the acknowledgment of the role of content dissemination by platforms.

The consideration of the General Data Protection Regulation and related legal acts in the field of data protection law is relevant, as it pursues both a cross-sectorial approach, which all data processors must follow in principle, and a cross-border approach, which links to the consumers of services made available online and thus also addresses providers who are not established in the EU. In addition, the particularly differentiated and far-reaching harmonised provisions on supervisory structures serve as an example for the presentation of a new, very far-reaching harmonisation approach at EU level, which is otherwise unfamiliar to regulation in the media sector.

2.4.1. e-Commerce Directive

Adopted in 2000, the ECD was intended to create for the first time a coherent framework for Internet commerce. The core of the Directive is to eliminate legal uncertainties for cross-border online services and to ensure the

free movement of information society services between the Member States.[194]

2.4.1.1. Historical Background

Already in April 1997, in the context of its Communication "A European Initiative in Electronic Commerce", the Commission identified an urgent need to engage in an early political debate with the aim to provide a stimulus to electronic commerce.[195] Driven by the "Internet Revolution", electronic commerce, as a rapidly developing sector, would have a major impact on Europe's competitiveness on the global market. Regulatory measures should therefore ensure that fragmentation of this promising market is avoided and that the benefits of the further development of information and communication technology, the liberalisation of telecommunications markets, the introduction of the euro and the internal market are exploited.

The main focus of the Communication was on economic aspects. The Commission referred to estimates that the value of Internet transactions could reach up to ECU[196] 200 billion in 2000. The proposed actions therefore aim to "provide a stimulus to electronic commerce and to avoid a fragmentation of this promising market". However, the Commission does not address concrete regulatory proposals. In particular, no statement is made on a possible design of the liability system in the e-commerce sector. A legal framework based on the initiative should, in particular, offer coherent regulation that encourages companies to invest in appropriate products, services and infrastructure and which gives consumers the opportunity to gain confidence. This should ensure that the global and European legal frameworks fit together. A number of other issues should also be addressed in this context. The Communication identifies areas such as data protection, protection of intellectual property rights, data security and a clear and neutral tax environment.

---

194 The provisions of the ECD relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382, II. A.

195 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, A European Initiative in Electronic Commerce, COM(97)157 final, p. 4.

196 The European Currency Unit (ECU) was a basket of the currencies of the European Community Member States, used as the unit of account of the European Community before being replaced by the euro on 1 January 1999.

However, the Communication was already assuming a broad regulatory framework at this stage. "Electronic Commerce", for example, defines all electronic business activities of companies among themselves, with their customers or with the administration. This includes both so-called indirect electronic commerce, i.e. the electronic ordering of tangible goods even when physically delivered, as well as direct electronic commerce, i.e. the online ordering, payment and delivery of intangible goods and services such as computer software, entertainment content or information services.

On 18 November 1998, a first proposal for the ECD was submitted, shortly after the Digital Millennium Copyright Act[197], which incorporated a similar liability regime as the later ECD, was signed in the U.S.[198]

As key areas of regulation, the proposal identifies the responsibility of intermediaries, electronic contracts, commercial communications, transparency and enforcement, and the country-of-origin principle. In particular, the chosen framework should be simple, minimalist and predictable.[199] The primary objective of the liability rules is to prevent distortion of competition between cross-border services through different civil and criminal responsibilities. Similar to the Directive adopted later, providers are therefore not responsible as long as they merely act as intermediaries for information provided by third parties.

> *(16) Whereas, both existing and emerging disparities in Member States' legislation and case-law concerning civil and criminal liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; whereas service providers have a duty to act, under certain circumstances, with a view to preventing or ceasing illegal activities; whereas the provisions of this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; whereas such mechanisms could be developed on the basis of voluntary agreements be-*

197 The Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

198 *Weidert/Molle*, in: Ensthaler/Weidert, p. 396 para. 39; regarding DCMA and ECRL see also *Freytag*, MMR 4/1999, p. 207, 207 et seq.

199 As described in the Report on the proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market (COM(98)0586 – C4-0020/99 – 98/0325(COD)), Committee on Legal Affairs and Citizens' Rights, under point B. Explanatory Statement, 1. Introduction.

> *tween all parties concerned; whereas it is in the interest of all parties involved in the provision of Information Society services to adopt and implement such procedures; whereas the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification;*[200]

The European Parliament occasionally expressed concern about a too broad limitation of liability and the impact of harmful content on the Internet.[201] In principle, however, the rules proposed in Art. 12–14 were seen as achieving an appropriate balance between the interests of potential rights holders and intermediaries during the discussion at the time.

Following a further draft[202], the Council's General Approach of 28 February 2000 was approved by the European Parliament and the Directive was published on 17 June 2000.

The Directive establishes the freedom to provide information society services (ISS) throughout the EU on the one hand and harmonises national rules on transparency and information obligations for online service providers, liability limitations and obligations for intermediaries on the other. The specific scope of the Directive covers "information society services". For that matter, it refers to the definition as laid down in the so-called Technical Standards Transparency Directive[203]. According to this it is any service normally provided for remuneration, at a distance, by elec-

---

200 Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, COM/98/0586 final, Recital 16.

201 Opinion for the Committee on Legal Affairs and Citizens' Rights on the proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market (COM(98)0568 – C4-0020/99 – 98/0325(COD)) (report by Ms Oddy), Committee on Culture, Youth, Education and the Media, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1999-0248+0+DOC+XML+V0//EN.

202 Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market, COM/99/0427 final, OJ C 248 E, 29.08.2000, pp. 69–96.

203 Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 217, 5.8.1998, pp. 18–26, as repealed by codified Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services OJ L 241, 17.9.2015, pp. 1–15.

tronic means and at the individual request of a recipient of services. Thereby, the term covers a wide range of economic online activities, including those that are financed, for example, by advertising.[204] Art. 1 para. 5 ECD explicitly excludes the areas of taxation, data protection, cartel law and gambling. With reference to the example of the Television without Frontiers Directive[205], the ECD is intended – in its words – to achieve a high level of Community integration in order to make full use of the opportunities offered by the internal market.[206]

At the same time, the free movement of ISS is understood as a manifestation of the right to freedom of expression within the meaning of Art. 10 para. 1 ECHR.[207] The Directive follows the main features already mentioned in the 1997 Communication of a light and flexible regulatory framework ("light touch approach"), a technology-neutral and horizontal design and a comprehensive scope applicable to both B2B and B2C relations.[208]

2.4.1.2. Further Developments

Since the adoption of the ECD almost 20 years ago, no reform of the Directive has been proposed, although the implementation of the ECD has been reviewed/evaluated several times. In addition, the provisions of the ECD have been supplemented over time by a number of sectorial Directives and Regulations relating to individual sub-areas and by a number of Recommendations and Communications from the Commission, which refer to the ECD but leave the Directive untouched in its scope.

Art. 21 ECD provides for a regular review of the implementation of the rules and their technical and economic circumstances. In 2003, the Commission presented its first report on the application of the Directive to the

204 ECD, Recital 18.
205 Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities.
206 ECD, Recital 4.
207 ECD, Recital 46.
208 *Valcke/Dommering*, in: Castendyk/Dommering/Scheuer, European Media Law, p. 1084.

European Parliament, the Council and the Economic and Social Committee.[209]

According to the report, the Directive already achieved "substantial and positive effects" by applying the internal market principle and the freedom to provide services to electronic commerce. However, the report also stressed that, in view of the continuing technological innovation and the rapid growth of electronic commerce, the Commission should keep a close eye on the application of the Directive. With regard to the liability of intermediaries, the Commission emphasises the regime applicable under the Directive. The liability rules would be limited to what is strictly necessary and essential both to ensure the provision of basic services and to create a framework that would provide possibilities for the Internet and e-commerce to develop. However, the use of a general policy to combat illicit content on a larger scale, and not merely in the case of specific infringements, would give rise for concern.

In 2007, the Commission commissioned two studies on the legal and economic impact of the ECD.[210] In particular, the "Study on the liability of Internet intermediaries" examined the legal framework and the jurisprudence on liability limitations under the ECD until 2007. As specifically problematic areas the authors identified the enforcement of orders to filter and block illegal content along the different interpretation of the requirement of "knowledge" by intermediaries and the measures to disclose customer data in order to prosecute infringements.

In addition, in 2011 and 2012, two public consultation procedures, taking into account economic matters and the procedure regarding illegal content, were carried out by the Commission.[211] Further studies were inter alia commissioned by the European Parliament. One example is a study

209 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee – First Report on the application 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 (Directive on electronic commerce), COM/2003/0702 final.

210 *Verbiest/Spindler/Riccio*, Study on the Liability of Internet Intermediaries; and *Nielsen and others*, Study on the Economic Impact of the Electronic Commerce Directive.

211 Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC); Public Consultation on the Procedures for notifying and acting on illegal content hosted by online intermediaries, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42071.

carried out at the request of the European Parliament's Committee on the Internal Market and Consumer Protection (IMCO), inquiring the extent to which Internet intermediaries should be held liable in future for the illegal activities of their users.[212]

As mentioned above, the broad regulatory approach of the ECD was supplemented by various sector-specific rules, for instance in the area of consumer protection law.[213] Most recently, as part of the Strategy for a Digital Single Market for Europe, several e-commerce-related rules were adopted or announced, such as a revised Payment Services Directive[214], new rules to prevent unjustified geo-blocking[215], revised consumer protection rules[216] and new VAT rules for the online sale of goods and services[217].

---

212 Cf., e.g., *van Eecke/Truyens*, Legal analysis of a Single Market for the Information Society; *Sartor*, Providers Liability: From the eCommerce Directive to the future.

213 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 304, 22.11.2011, pp. 64–88.

214 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, pp. 35–127.

215 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 60I, 2.3.2018, pp. 1–15.

216 Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM/2018/0184 final; Proposal for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules, COM/2018/0185 final.

217 Council Directive (EU) 2017/2455 of 5 December 2017 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods, OJ L 348, 29.12.2017,

In addition, the Commission adopted recommendations and communications on complementing the rules on electronic commerce. These include, for example, the Commission's 2012 Communication regarding "A coherent framework for building trust in the Digital Single Market for e-commerce and online services"[218] on the potential of online services for growth and jobs and the more recent Recommendations on measures to effectively tackle illegal content online.[219]

Without fundamentally abandoning the principle enshrined in the ECD that Internet service providers acting as intermediaries are not liable for the content they transmit, store or make available, the Commission, already in its Communication on the Strategy for a Digital Single Market for Europe and in light of combatting illegal online content, noted that, given the growing amount of digital content available on the Internet, "today's rules are likely to come under increasing pressure". Against this backdrop, a trend towards greater responsibility, especially for platform operators, can be observed beyond soft law instruments, particularly in the context of the recently adopted reform of copyright law in the Digital Single Market and the proposal for a Regulation on preventing the dissemination of terrorist content online[220].

In her political guidelines for the period 2019 to 2024, Commission President designate Ursula von der Leyen announced that she will enact a new Digital Service Act to update the Union's liability and safety rules for digital platforms, services and products.[221]

---

pp. 7–22; Council Regulation (EU) 2017/2454 of 5 December 2017 amending Regulation (EU) No 904/2010 on administrative cooperation and combating fraud in the field of value added tax, OJ L 348, 29.12.2017, pp. 1–6.

218 Commission Communication to the European Parliament, the Council, The Economic and Social Committee and the Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM/2011/0942 final.

219 Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ 2018 L 63/50; cf. on this in detail Chapter 2.5.2.

220 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19–20 September 2018, COM/2018/640 final.

221 Political guidelines for the next Commission (2019–2024), "A Union that strives for more: My agenda for Europe", 16 July 2019.

2.4.1.3. Main Goals and Principles of the Original ECD

The adoption of the ECD was justified on grounds of legal obstacles that hindered the free exercise of internal market principles, in particular, the right of establishment (Art. 49 TFEU)[222] and the freedom to provide services (Art. 56 TFEU)[223]. Recital 5 ECD mentions a number of obstacles, such as the divergent national rules concerning information society service providers and the extent to which Member States may control services originating from another Member State.

The ECD functions in accordance with the principle of proportionality. The details of this approach are laid down in Recital 10. The ECD limits itself to regulating only those legal aspects and matters that pose problems for the functioning of the internal market. In that respect, the Directive pursues a minimum harmonisation approach. This means that the ECD approximates the rules applicable to information society services only to the extent that obstacles to the free operation of the internal market are to be removed and the general interest principles are to be safeguarded, in particular the protection of minors, consumers and public health. Generally speaking, for ISS as defined in the Technical Standards Transparency Directive – mentioned above – the basic idea was that Member States are barred from introducing a prior authorisation request. But in order to make the single market function the basic idea is that there is one jurisdiction and the responsible Member States ensure an effective supervision. Besides some rules informing the users better about the identity of the providers, the most important element was the introduction of a liability (exemption) regime, which has had significant impact on the topics covered by this study. Further, there are only limited rules on supervision or enforcement, but Art. 18 ECD does foresee that, e.g., States need to ensure that there are efficient court procedures that allow for termination of infringements and prevention of further impairments of the interests of the concerned parties.

Art. 1 para. 2 ECD defines the areas affecting information society services which, according to the EU at the time, necessitated regulatory intervention. Necessary areas for action were Member State provisions concerning the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct,

222 Ex-Art. 43 of the Treaty of the EC (TEC).
223 Ex-Art. 49 TEC.

out-of-court dispute settlements, court actions and cooperation between Member States.

At the same time, the ECD complements the legislative body of the EU Consumer acquis. Where its provisions affect other rules laid down in this body of EU law, the Directive may enhance them but shall not diminish the level of protection, in particular where it concerns public health and consumer interests. Against that background, Recital 11 of the ECD refers to EU legislation (at the time) that needs to be taken into account. Some of the more substantial provisions referred to were the Council Directive 93/13/EEC on unfair terms in consumer contracts, Directive 97/7/EC on the protection of consumers in respect of distance contracts[224], Directive 84/450/EEC concerning misleading advertising[225] and Directive 92/59/EEC on general product safety.[226]

The Directive does not affect national or Community measures that promote cultural and linguistic diversity and measures to defend pluralism. Finally, Recitals 63 and 64 underline that the Directive should not stand in the way of Member States' efforts to utilise the means provided by electronic communications for the attainment of social, democratic and cultural goals.

The minimum harmonisation approach also plays out in the choice of regulatory tools favoured by the EU legislator in this field. In order to minimise regulatory intervention, the ECD emphasises the use of self-regulatory measures, such as codes of conduct. This is important in the more recent context when discussing the role of the Commission in establishing processes and agreements with industry to fight unlawful content online, which will be discussed further below. Recital 32 and Art. 16 encourage Member States to promote and create voluntary codes of conduct through the involvement of industry and professionals. In addition, Art. 17 promotes the use of out-of-court dispute settlements.

---

224 Replaced by Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, pp. 64–88.

225 Replaced by Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, OJ L 376, 27.12.2006, pp. 21–27.

226 Replaced by Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002, pp. 4–17.

2.4.2. Audiovisual Media Services Directive

2.4.2.1. Historical Development up to the Latest Revision in 2018

The AVMSD in its current version is based on a three decades long evolution during which it has been repeatedly adapted to current market conditions as well as technical and social developments.[227] The foundation for a common market for cross-border television was established at European level 30 years ago with the Television without Frontiers Directive (TwFD)[228]. On the one hand, the agreement of minimum conditions which applied to every television broadcaster under the jurisdiction of a Member State of the European Economic Community (now the European Union) and, on the other hand, the country-of-origin principle, according to which only one Member State shall be responsible for regulating a broadcaster, formed the core of the TwFD. Broadcasters were permitted to broadcast throughout Europe without any further control if the national legal requirements were complied with. The Directive is still based on these basic principles, which are as relevant today as they were when it was adopted.[229] Nevertheless, the Directive has been revised once every decade.

In an effort to adapt the provisions of the TwFD to a new advertising environment and to the technological developments in the field of television broadcasting, Directive 1997/36/EC[230] introduced, inter alia, provisions on the regulation of teleshopping, clarified the rules on jurisdiction (the Member State responsible for television channels is determined by the location of the head office and the place where programming decisions are made) and deepened rules on the protection of human dignity. Moreover, a Contact Committee to monitor the implementation of the Directive and the developments in that sector, and a forum for the exchange of views

227 Cf. on this and this Chapter overall: *Weinand*, Implementing the EU Audiovisual Media Services Directive.

228 Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities, OJ L 298, 17.10.1989, pp. 23–30.

229 Cf. in particular on the country-of-origin principle: *Cole*, The Country of Origin Principle.

230 Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, OJ L 202, 30.7.1997, pp. 60–70.

were established under the Directive. Furthermore, the revised Directive placed greater emphasis on the protection of minors by specifying, for example, that Member States must ensure that programs which are likely to impair the development of minors and are broadcast in unencrypted form are to be preceded by an acoustic warning or identified by a visual symbol.

However, the most significant changes (also in the context of this study) until the AVMSD's most recent revision were those introduced in 2007. Directive 2007/65/EC[231] adapted the provisions to the new technical environment, generated by the growing importance of the Internet, and thus took account of the increasing convergence of the media. Accordingly, the Directive was given its current name, which no longer focused solely on "television without frontiers" but also on audiovisual media services. In addition to redefining the provisions on responsibility against the background of the country-of-origin principle and the consideration of self- and co-regulation mechanisms, the rules on cooperation between regulators and the implementation of provisions for on-demand services were the most significant innovations.

While the Contact Committee had already been set up with the 1997 reform, the revised Directive from 2007 took a further step with the adoption of Art. 23a, according to which Member States shall take appropriate measures to provide each other and the Commission with the information necessary for the application of the provisions of the AVSMD. The entry into force of that provision was crucial, in particular, due to the fact that cross-border content became more and more relevant.[232] In 2014, Art. 23a built the basis for the establishment of the European Regulators Group for Audiovisual Media Services (ERGA), which should serve as an advisory body to the Commission in its implementation of activities concerning areas coordinated by the AVMSD and which should facilitate coordination and cooperation between the national regulatory bodies in the Member States. In its decision establishing the ERGA, the Commission outlined, inter alia, that, "[i]n order to achieve a successful development of an internal market for audiovisual media services notably in view of increased cross-border dissemination and the regulatory challenges linked to on-demand

231 Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, OJ L 332, 18.12.2007, pp. 27–45.

232 Cf. Recitals 32 and 66 of Directive 2007/65/EC.

services", a coherent application of the AVMSD in all Member States is essential and that "[t]o achieve this goal it is crucial to facilitate a closer and more regular cooperation between the competent independent regulatory bodies of the Member States and the Commission"[233].

Considering that legal uncertainty and a non-level playing-field exist for European companies delivering audiovisual media services as regards the legal regime governing emerging on-demand audiovisual media services, the competent EU institutions also found it necessary that, in order to avoid distortions of competition, to improve legal certainty, to help complete the internal market and to facilitate the emergence of a single information area, at least a basic tier of coordinated rules applies to all audiovisual media services, both television broadcasting and on-demand audiovisual media services (cf. Recital 7). However, the basic principles of Directive 89/552/EEC, namely the country-of-origin principle and common minimum standards, had proved their worth and therefore were retained. While the ECD, which had already been in force for five years at the time of the Commission's AVMSD reform proposal at the end of 2005, dealt with the much broader spectrum of electronic commerce and addressed information society services, the scope of AVMSD, which has always been primarily related to the function of (cross-border) television to protect the general interest[234], had to be adjusted. Therefore, the definition established for audiovisual media services covered mass media only in their function to inform, entertain and educate the general public. Any form of private correspondence, services whose principal purpose is not the provision of programs (e.g. websites that contain audiovisual elements only in an ancillary manner, such as animated graphical elements, short advertising spots or information related to a product or non-audiovisual service), games of chance involving a stake representing a sum of money, including lotteries, betting and other forms of gambling services, online games and search en-

233 Commission Decision of 3.2.2014 on establishing the European Regulators Group for Audiovisual Media Services, C(2014) 462 final, available at https://ec.europa.eu/digital-single-market/en/news/commission-decision-establishing-european-regulators-group-audiovisual-media-services, p. 2, Whereas (3).

234 Cf. already the considerations in the TwFD: "Whereas broadcasts transmitted across frontiers by means of various technologies are one of the ways of pursuing the objectives of the Community; whereas measures should be adopted to permit and ensure the transition from national markets to a common programme production and distribution market and to establish conditions of fair competition without prejudice to the public interest role to be discharged by the television broadcasting services; […]."

gines were excluded from the scope of the AVMSD as were electronic versions of newspapers and magazines, private websites and services consisting of the provision or dissemination of audiovisual content generated by private users for the purposes of sharing and exchange within communities of interest.[235] Thus, only audiovisual content produced and provided with a certain level of editorial responsibility (to be further defined by the Member States) was covered, whereas the ECD, for example, covered *any* service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient. With the extension of the scope to include on-demand services in the online environment on the one hand and the restrictive definition on the other, both the convergence of the media was taken into account and the fact that audiovisual services in particular are the focus of harmonisation because of their increased suggestive power.[236]

For reasons of clarity and rationality, the Directive was subsequently codified in order to incorporate the three amending Directives into a new single text, Directive 2010/13/EU.[237]

In 2013, the Commission published a Green Paper on "Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values"[238], which gave a major boost to the process of reforming the audiovisual sector again. The Green Paper should launch a broad public debate on the impact of the change in the audiovisual media landscape, which is characterised by an ever-increasing convergence of media services and the way these services are used and delivered, and on the impact of the borderless Internet in particular on market conditions, interoperability and infrastructure. The Commission received a number of submissions in the con-

235 Cf. Directive 2007/65/EC, Recital 16 et seq.

236 Cf. on the suggestive power of audiovisual media the report by Andreas Grünwald on possible options for the review of the European Convention on Transfrontier Television: Standing Committee on Transfrontier Television of the Council of Europe, Doc. TTT(2003)002, 24 April 2003.

237 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ L 95, 15.4.2010, pp. 1–24, and the Corrigendum to Directive 2010/13/EU, OJ L 263, 6.10.2010, pp. 15–15.

238 Opinion of the European Economic and Social Committee on the 'Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values (Green Paper)' COM(2013) 231 final, OJ C 341, 21.11.2013, pp. 87–91.

sultation procedure it launched[239] as well as expressions from other EU institutions, notably from the European Parliament[240] and the Council[241]. In particular, the need for a renewed adaptation of the AVMSD rules to the ongoing convergence of the media was stressed in the several opinions, emphasising that the horizontal (sector convergence), vertical (value chain convergence) and functional convergence (convergence of applications/services) all impact the audiovisual industry and that technical convergence means that media law and network policy issues are increasingly overlapping.[242] Some even argued that any de-regulation of the current services within the scope of the AVMSD would need to look at the growing asymmetry between media companies, media platforms and media aggregators in both the regulatory and fiscal playing fields.[243] Consequently, in 2015 the European Commission explicitly announced in its Strategy for a Digital Single Market that it would review the AVMSD with regard to its scope and the nature of the rules applicable to all market players, in particular the measures to promote European works, the rules on the protection of minors and the advertising rules.[244]

All this led to a reform proposal by the European Commission in 2016 amending Directive 2010/13/EU on the coordination of certain provisions

239 The results of the consultation on the Green Paper are available at https://ec.europa.eu/digital-single-market/en/news/consultation-green-paper-preparing-fully-converged-audiovisual-world-growth-creation-and-values.

240 European Parliament resolution of 12 March 2014 on Preparing for a Fully Converged Audiovisual World (2013/2180(INI)), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0232+0+DOC+XML+V0//EN.

241 Council conclusions on European Audiovisual Policy in the Digital Era Education, Youth, CULTURE and SPORT Council meeting Brussels, 25 November 2014, available at https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/educ/145950.pdf.

242 Cf. European Parliament resolution of 12 March 2014, loc. Cit. (fn. 240), para. C. and D.

243 Cf. Commission, summaries of the replies to the public consultation launched by the Green Paper "Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values", available at https://ec.europa.eu/digital-single-market/en/news/publication-summaries-green-paper-replies, p. 40; in this context it was even outlined that "[i]t is at this juncture that an evaluation of the crossover between AVMSD and the eCommerce Directive would be necessary".

244 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192, para. 3.2.

laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, which finally resulted in the amending Directive (EU) 2018/1808 after an intensive two-year trilogue procedure.[245] Member States must transpose the reformed rules into national law by 19 September 2020.

The importance of this last reform lies, among other things, in the further extension of its scope: while audiovisual media services and their providers remain the focus and starting point of the Directive, certain types of distributors are now also addressed. This applies directly to video-sharing platforms, which have been included in the scope of the Directive and will be given greater responsibility under the new provisions (in particular Art. 28b). The extension has taken place mainly in the light of the fact that more or less new players on the market are competing with traditional service providers, such as television, for the attention of the same recipients and the same advertisers (Recital 4). This shows similarities to the inclusion of VoD offers within the framework of the 2007 reform but goes beyond the adaptation of the former rules, to the extent that the feature of television-likeness, which still played a role at that time regarding VoD services, is now dispensed. Whereas previously the (partly) harmonisation of the legal framework was based on a similarity of formats, the current approach is more based on similarities with regard to the audience concerned.[246] In the future, VSP providers will have to follow the same rules as other audiovisual media service providers with regard to sponsorship, product placement, surreptitious advertising, subliminal influence, and tobacco and alcohol advertising. Only the consequence of the applicability of the rules is different from that of linear and non-linear providers, which here also depends on the question of the economic advantage of the VSP provider. In their dealings with users, VSP providers merely have to push for compliance with the legal requirements by means of suitable measures, whereas they have to ensure compliance with their own commercial communication in a binding manner. Art. 28b also establishes a catalogue of obligations to be observed by VSP providers in order to protect both minors and the general public from certain harmful content, including, for example, the establishment of age verification mechanisms, reporting and

245 For a detailed overview on the trilogue procedure cf. the different synopses of the EMR, available at https://emr-sb.de/gb/synopsis-avms/.

246 On this and the following see *Cole/Etteldorf*, in: Medienhandbuch Österreich 2019, p. 56, 57 et seq.

complaint systems. In order to implement those objectives, Member States should support the use of co-regulation and the promotion of self-regulation through codes of conduct – an instrument that has taken on much greater overall weight with the reform of the Directive.

Indirectly, however, some rules of Directive (EU) 2018/1808 also affect other platforms that make audiovisual content accessible. This applies in particular to the new rules on searchability and signal integrity of audiovisual content (Art. 7a and 7b), which oblige Member States to take measures to ensure the appropriate prominence of audiovisual media services of general interest and require that audiovisual media services provided by media service providers are not, without the explicit consent of those providers, overlaid for commercial purposes or modified.

Finally, the legal framework for non-linear service providers has been (partially) aligned with the previous legal framework for linear services. This is the case in the areas of the promotion of European works and the protection of minors in the media, where Art. 6a introduced a provision that applies to all media service providers.

The historical development of the former TwFD shows that, over time, the Directive has been constantly adapted to new technical and social developments. Media convergence has been identified and addressed. Particularly noteworthy are the aforementioned rules on searchability and overlay protection, as they document the AVMSD's efforts to ensure a comprehensive protection of audiovisual content, the consequences of which go beyond the actual core area of application and also include access to other providers like distributors. At its core, however, the AVMSD still deals with the regulation of cross-border audiovisual content, which is an important part of the European structure against the background of the creation of a Digital Single Market. The AVMSD's regime is thus subject to equal limits, both in terms of its scope of application outside audiovisual media service providers and in terms of enforcement. The possibilities and limits arising from this (also for the national regulatory authorities) will be examined in the following section.

2.4.2.2. Overview of Relevant Rules for the Online Context

2.4.2.2.1. Personal Scope of Application

The AVMSD[247] initially covered two types of services in particular: audiovisual media services within the meaning of Art. 1 para. 1 lit. a and video-sharing platforms within the meaning of Art. 1 para. 1 lit. aa AVMSD.

The first term covers both audiovisual commercial communications and services (linear and non-linear) as defined by Art. 56 and 57 TFEU, where the principal purpose of the service or a dissociable section thereof is devoted to providing programs, under the editorial responsibility of a media service provider, to the general public in order to inform, entertain or educate by means of electronic communications networks within the meaning of lit. a of Art. 2 of Directive 2002/21/EC. In the online sector, the definition covers, for example and above all, streaming offers or media libraries of traditional broadcasters as well as on-demand offers of other providers. However, individual channels or profiles on platforms such as Twitch or YouTube can also fall under this term if they are designed in the way that Art. 1 para. 1 lit. a describes.

Meanwhile, with the 2018 reform, a separate definition was created for abovementioned platforms that base their business models on the fact that their users themselves create the content to make it available via the platform. According to Art. 1 para. 1 lit. aa, video-sharing platform service means a service as defined by Art. 56 and 57 TFEU, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate by means of electronic communications networks within the meaning of lit. a of Art. 2 of Directive 2002/21/EC, whereby the organisation of such providing is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.

Although there are many criteria in this definition that should characterise a VSP covered by the AVMSD, the definition is very broad. For example, there is no exception for small platform providers as in the new

247 The provisions of the AVMSD relevant in the context of this study are reprinted in the Online Annex to this study, available at www.nomos-shop.de/44382, II. B.

DSM Directive.[248] Rather, the size or economic power of a platform is only taken into account within the framework of the measures that the provider has to take to implement the requirements of the AVMSD. This means that not only large platforms such as YouTube or Twitch, which was presumably the actual goal of the new rules, will be covered, but also smaller, national platforms such as the ones currently being set up in many Member States in the form of start-ups. In addition, there is no restriction to specific content, which means that niche-specific offers such as pornography platforms with user-generated videos or (audiovisual) forums of a themed community (e.g. websites with do-it-yourself instructions or videos on pet education) have to comply with the new rules, too. Finally, the scope is not limited to "audiovisual platforms" alone. This is emphasised in the Recitals to the AVMSD mentioning in particular "social media services" (Recital 4) and "electronic versions of newspapers and magazines" (Recital 6). It is precisely in the area of such offers that the criterion of "essential functionality" will be of importance in future, for the assessment of which the Commission[249] has already announced that it will issue corresponding guidelines.[250]

As mentioned above, however, the 2018 AVMSD reform also introduced provisions that do not directly address other platform providers in the sense of (also definitory) including them within the scope of the Directive but indirectly affect the structure of their offerings. This applies in particular to the provisions of Art. 7a and b AVMSD. According to those provisions, Member States may take measures to ensure the appropriate prominence of audiovisual media services of general interest and shall take appropriate and proportionate measures to ensure that audiovisual media services provided by media service providers are not, without the explicit consent of those providers, overlaid for commercial purposes or modified. At the core of these provisions are the content providers whose content is to be protected and made retrievable, as well as the users to whom the content is to be made easily accessible and who are nevertheless to remain in control of certain functions.[251] However, the implementation of these re-

248 Art. 17 para. 6 of DSM Directive.

249 Cf. the report of the Commission of 21.3.2019 on the preparatory work for AVMSD guidelines, available at https://ec.europa.eu/digital-single-market/en/news/preparatory-work-avmsd-guidelines-report-stakeholder-workshop.

250 Cf. on this also *Kogler*, in: K&R 9/2018, p. 537, 540; *Cole*, AVMSD Jurisdiction Criteria after the 2018 Reform.

251 Cf. on this *Cole*, Die Neuregelung des Artikel 7b Richtlinie 2010/13/EU (AVMD-RL).

quirements into national law must nevertheless address the providers of these platforms, as only they can ensure that these offerings are easy to find and that they are protected against overlays by designing them accordingly. How the Member States transpose the rules on taking "appropriate and proportionate" measures (in compliance with fundamental rights and primary law requirements) is in principle up to them. Not least because of the indeterminate legal terms "media services of general interest" or "legitimate interests of users", which exist in these regulations and which can be concretised by the Member States through laws of the legislator or guidelines of the regulatory authorities, it is to be expected that a uniform implementation throughout the EU will not take place in this area either. This is all the more true in view of the fact that the Member States also have at their disposal the instruments of self- and co-regulation.

2.4.2.2.2. Country-of-Origin Principle

2.4.2.2.2.1. Importance of the Principle and Changes Related to It in the Recent Reform

The core principle of the AVMSD and its predecessor, the TwFD, has always been the country-of-origin principle, which determines the regulatory approach towards providers of linear and non-linear audiovisual media services. This principle laid down in Art. 2 para. 1 AVMSD states that a provider that falls under the jurisdiction of one EU Member State can rely on complying with the legal framework of (only) that specific state in order to be authorised to disseminate content across all EU Member States. Art. 2 para. 3 and 4 thereby lays down under which circumstances jurisdiction can be assumed. The flipside of this approach was to ensure that a certain number of key issues relevant for all Member States would be harmonised by the Directive, in which way they would become the minimum standard that is respected across the EU.[252] In the online context, therefore, the country-of-origin principle is linked in particular to the minimum harmonisation of audiovisual content (Chapter 2.4.2.2.3).

Although this was problematised[253] within the framework of the reform, the country-of-origin principle was retained in its entirety in the AVMSD when it was reformed in 2018. Only minor changes were made to

252 *Cole*, AVMSD Jurisdiction Criteria after the 2018 Reform, p. 5.
253 Cf. *Kogler*, in: K&R 9/2018, p. 537.

the jurisdiction criteria.[254] Furthermore, and what is particularly relevant in the context of this study, Art. 3 AVMSD, which contains rules and exceptions regarding the country-of-origin principle, has been amended. This concerns in particular the harmonisation of the rule on linear and non-linear services and the streamlining of the procedure before the European Commission (Art. 3 para. 6).

As can be seen in detail from the synoptic illustration of the provisions of Art. 3 before and after the 2018 reform in the annex[255], there have been some significant changes here. This applies in particular to the harmonisation of the provisions for linear and non-linear providers in this area. While Art. 3 para. 4 of Directive 2010/13/EU still contained a special provision for taking (not only in the case of linear services temporary) measures against non-linear offers, which almost identically adopted the wording of the corresponding possibility of deviation from the country-of-origin principle from the ECD (Art. 3 para. 4), Art. 3 para. 4 has now given way to uniform regulation under Art. 3 para. 2 and 3, which no longer continues the synchronisation between AVMSD and ECD in this area. Art. 3 para. 2 and para. 3 apply to all audiovisual media services and distinguish, other than before, according to the type of infringement, although in both cases only temporary measures may be imposed by the Member States. The strict distinction between violations of Art. 6 para. 1 lit. a and Art. 6a para. 1 (in Art. 3 para. 2 AVMSD), on the one hand, and Art. 6 para. 1 lit. b and other state interests (in Art. 3 para. 3 AVMSD), on the other, appears only in its current form in the final compromise proposal, while the Commission's proposal still contained an overall uniform rule.[256] The decisive difference between the two provisions is essentially that Art. 3 para. 2 requires a twofold violation of the provisions mentioned therein for action to be taken, while under Art. 3 para. 3 AVMSD a one-time violation is sufficient for Member States to impose measures.

254 For a detailed overview and a genesis of the provisions cf. *Cole*, AVMSD Jurisdiction Criteria after the 2018 Reform.

255 Online Annex, available at www.nomos-shop.de/44382, II.B.

256 Cf. on this the synopsis provided by the EMR giving an overview on the trilogue, available at https://emr-sb.de/wp-content/uploads/2019/03/EMR-Synopsis-AVMSD_final_EN.pdf.

2.4.2.2.2.2. Home State Jurisdiction Rule

Art. 3 para. 1 states that a media service provider always has the right to retransmit its content to other EU Member States without any restriction being imposed by the state receiving such a retransmission. However, there are possible exceptions to this obligation as well as a safeguard mechanism to avoid a "race to the bottom" through what is known as "forum shopping": if specific violations of the Directive do not lead to measures imposed by the supervisory authority in the country of origin, authorities in the receiving state can derogate from the retransmission requirement, subject to a procedure laid down in the Directive. Furthermore, in the case of linear services, it may under certain circumstances be assumed that a provider that transmits from abroad but only targets an audience in the home country is circumventing the latter's laws, and the relevant supervisory authority may then take action.[257]

The country-of-origin principle and thus the fundamental guarantee of freedom of reception under Art. 3 para. 1 AVMSD only apply in the area coordinated by the Directive. However, in the area of cross-border distribution of (audiovisual) content online, which is relevant in the context of this study, there are hardly any conceivable areas where coordination can be completely neglected by the Directive (in particular with regard to the protection of minors from harmful media, protection against violence and hatred, and terrorist content). The CJEU, too, has so far been rather cautious on this point. In the *Commission v Belgium*[258] case, for example, the Court rejected a reference to cultural policy objectives, in particular the safeguarding of pluralism and the protection of morality, public order and public security, and a reference to a lack of coordination by the Directive, since at least part of the area was coordinated. In the *De Agostini* case, the CJEU left an appeal to consumer protection principally open, as this area was not fully coordinated at EU level (at that time), but denied that possibility with regard to the protection of minors.[259]

In this context, a recent decision of the CJEU on the scope of Art. 3 para. 1 AVMSD requires particular attention. In its judgment of 4 July

257 Cf. on this and the following also *Cappello (ed.)*, Media law enforcement without frontiers, IRIS Special 2018-2.

258 CJEU, judgement of 10.9.1996, C-11/95, *Commission of the European Communities v Kingdom of Belgium*.

259 CJEU, judgements of 09.7.1997, joint cases C-34/95, C-35/95 and C-36/95, *Konsumentombudsmannen (KO) v De Agostini (Svenska) Förlag AB and TV-Shop i Sverige AB)*, para. 57 et seq.

2019, the Court ruled in the *Baltic Media Alliance* case[260] that the AVMSD does not preclude a provision in Member State legislation which allows for a temporary obligation to transmit or retransmit a television channel from another Member State only in form of pay-TV packages. This could be lawful for reasons of public order such as combating incitement to hatred. The CJEU thus ruled in favour of the Lithuanian Radio and Television Commission (*Lietuvos radijo ir televizijos komisija*, LRTK), which had issued a corresponding ruling to the Baltic Media Alliance. It had taken action against the United Kingdom-based television channel Baltic Media, which inter alia broadcasts the television channel NTV Mir Lithuania that is aimed at the Lithuanian public and contains predominantly Russian-language content. On the grounds that various broadcasts on the channel had incited hostility and hatred towards the Baltic States based on nationality, LRTK obliged the broadcaster to broadcast the channel NTV Mir Lithuania only in pay-TV packages for a period of twelve months. LRTK held that, in particular, the broadcasts targeted the Russian-speaking minority in Lithuania with false information about the collaboration of Lithuanians and Latvians in the Holocaust and alleged nationalist and neo-Nazi domestic policies of the Baltic States that ostensibly posed a threat to the Russian minority in the territories of these countries. The Court ruled that this does not constitute an obstacle within the meaning of Art. 3 para. 1 AVMSD if certain modalities – such as in this case the obligation to broadcast the channel only on pay-TV – do not prevent retransmission in the actual sense of the channel. Such a measure would not introduce a second check of the channel concerned in addition to the check to be carried out by the sending Member State, which is precisely what the country-of-origin principle seeks to prevent. Art. 3 para. 1 would only refer to the area coordinated by the AVMSD, which in turn is limited to the "provision of audiovisual media services". According to the CJEU, such interpretation may be derived from the wording and the history of that provision. Since the Court considered Art. 3 para. 1 to be irrelevant, it no longer found it necessary to examine Art. 3 para. 2 of the AVMSD in detail.

260 CJEU, judgement of 4.7.2019, C-622/17, *Baltic Media Alliance Ltd v Lietuvos radijo ir televizijos komisija*.

2.4.2.2.2.3. Exceptional Derogation of Free Flow of Information

Powers of the Member States to derogate temporarily from the principle of freedom of reception are found in Art. 3 para. 2 and 3 AVMSD. These rights apply when an audiovisual media service manifestly, seriously and gravely infringes Art. 6 para. 1 lit. a or Art. 6a para. 1 or prejudices or presents a serious and grave risk of prejudice to public health (Art. 3 para. 2 AVMSD) and when an audiovisual media service manifestly, seriously and gravely infringes Art. 6 para. 1 lit. b or prejudices or presents a serious and grave risk of prejudice to public security, including the safeguarding of national security and defence (Art. 3 para. 3 AVMSD). The relevant rules also set out further conditions and a specific procedure to be followed by the Member State concerned, involving the competent Member State, the Commission and the ERGA. The cooperation procedure provided for here makes it difficult in practice to take action against foreign providers, despite a possibility to derogate in urgent cases under Art. 3 para. 5 AVMSD.[261] This applies in particular against the background of the mentioned national peculiarities with regard to the interpretation of undefined legal concepts, the implementation of the provisions at national level and the distribution of responsibilities and competences regarding enforcement. If the Commission confirms conformity with Union law after the receiving state has notified the steps it has taken, "reception" of the content may be prevented. However, this does not include supervisory measures in form of direct enforcement measures addressed to the foreign provider but include rather possibilities to prevent the dissemination of offers, for instance by linking domestic infrastructure operators instead of imposing a fine.[262]

2.4.2.2.2.4. Exception in Case of Circumvention

Finally, the circumvention of Art. 4 para. 2 AVMSD, which applies to all audiovisual media services since the 2018 reform, should be mentioned.

261 Cf. the describing part and the country reports in: *Cappello (ed.)*, Media law enforcement without frontiers, IRIS Special 2018-2.

262 Cf. on this already *Ukrow*, Zur Zuständigkeit der Landesmedienanstalten/KJM für ausländische Anbieter, p. 193.

The provision codifies the relevant CJEU case-law on circumvention.[263] Where a Member State has exercised its freedom to adopt more detailed or stricter rules of general public interest (Art. 4 para. 1 AVMSD) and assesses that a media service provider under the jurisdiction of another Member State provides an audiovisual media service that is wholly or mostly directed towards its territory, it may request the Member State having jurisdiction to address any problems identified in relation to this paragraph. According to the requirements mentioned in Art. 4 para. 2, both Member States shall cooperate sincerely and swiftly with a view to achieving a mutually satisfactory solution. If a satisfactory solution is not found, the receiving Member State may adopt appropriate measures against the media service provider if, inter alia, it has adduced evidence showing that the media service provider in question has established itself in the Member State having jurisdiction in order to circumvent the stricter rules. But even this is only possible if a certain procedure has been followed (Art. 4 para. 4: the Commission and the competent Member State have been notified, opportunity to submit comments for the media service provider, Commission issued a decision on the compatibility with Union law, etc.).

Art. 4 serves as a backstop in cases when a provider has relocated to another Member State in order to avoid having to comply with stricter rules that a Member State has enacted while the provider was targeting mainly the territory of that Member State.[264] However, as Art. 4 constitutes an exception to a (fundamental) freedom, it needs to be interpreted narrowly.[265] The Commission sets a high threshold for evidence about a circumvention as it needs to be clearly distinguished from a "simple" use of the right to decide on establishment and profit from the country-of-origin principle which the Directive grants providers.[266]

---

263 For an overview cf. *Cole*, in: Fink/Cole/Keber, Europäisches und Internationales Medienrecht, para. 37 and 62.

264 Cf. on this *Cole*, AVMSD Jurisdiction criteria after the 2018 reform; *Cole*, The Country of Origin Principle, p. 120; *Herold*, in: Journal of Consumer Policy, 31(1), 2008, p. 5, 6.

265 Cf. Recital 43 of Directive 2010/13/EU and CJEU, judgement of 28.10.1999, C-6/98 *Arbeitsgemeinschaft Deutscher Rundfunkanstalten (ARD) v PRO Sieben Media AG, supported by SAT 1 Satellitenfernsehen GmbH, Kabel 1, K 1 Fernsehen GmbH*; on this *Cole/Haus*, in: JuS 5/2001, p. 435, 435 et seq.

266 Cf. Commission decision C(2018) 532 final, 31.1.2018, on the Swedish intention to impose a ban on alcohol advertising on two UK broadcasters which was considered as not compatible with EU rules.

2.4.2.2.3. Minimum Harmonisation Concerning Specific Types of Content

The minimum standards relevant in the context of this study, which audiovisual content must comply with also in the online sector, concern primarily the protection of minors, the protection against violence, hatred and terrorist content as well as the design of audiovisual commercial communication. Therefore, Art. 6, 6a and 9 of the AVMSD will be presented in the following, in particular the specifications which audiovisual media services must comply with, whereby VSP providers pursuant to Art. 28b para. 1 and 2 of the AVMSD (will) also meet corresponding requirements. This minimum harmonisation is the basis for cooperation between the regulatory authorities, since it contains a standard that all parties are obliged to maintain.

Directive 2010/13/EU	Directive (EU) 2018/1808
Art. 6	**Art. 6**
Member States shall ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to hatred based on race, sex, religion or nationality.	**1. Without prejudice to the obligation of Member States to respect and protect human dignity,** Member States shall ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any: (**a**) incitement to **violence or** hatred **directed against a group of persons or a member of a group based on any of the grounds referred to in Art. 21 of the Charter;** (**b**) **public provocation to commit a terrorist offence as set out in Art. 5 of Directive (EU) 2017/541.** **2. The measures taken for the purposes of this Art. shall be necessary and proportionate and shall respect the rights and observe principles set out in the Charter.**

Art. 6 AVMSD was significantly expanded with the 2018 reform. Member States shall ensure by appropriate, proportionate and necessary means that audiovisual media services do not contain incitement to violence or hatred against certain persons or groups of persons or public provocation to commit terrorist offences. While the provision on terrorist content is new, the incitement provision has been amended only in respect of the offences covered so as to extend to all grounds of discrimination referred to in Art. 21 of the CFR, thus achieving a more uniform approach in EU law

also in the formulation of prohibited grounds of discrimination. In addition to race, sex, religion or nationality (as in the past), the grounds of discrimination now include skin colour, ethnic or social origin, genetic characteristics, language, belief, political or other opinion, membership of a national minority, property, birth, disability, age and sexual orientation. Reference to Art. 21 CFR can also be found in a corresponding obligation for VSPs and may be seen as response to developments with regard to the exchange of discriminatory statements in online offers.[267]

Particularly noteworthy is the introductory sentence on human dignity, which not only emphasises that Member States have obligations derived from this fundamental right beyond the scope of Art. 6 AVMSD but also underlines the connection between Art. 6 AVMSD and considerations regarding human dignity. The additional ground of discrimination in connection with incitement to violence or hatred in Art. 6 para. 1 lit. a AVMSD limits the considerations made above on human dignity on the one hand, but on the other hand it also imposes an explicit obligation on the Member States in the sense of minimum harmonisation. When considering the emergence and growth of videos of populist associations within social networks or on VSPs, online content violating these requirements is probable.[268] Some Member States[269] have already addressed[270]the issue of hate speech at legislative level, independently of the provisions under Art. 6 AVMSD (and partly also independently of the limitation to audiovisual content), not without receiving strong criticism in view of the privatisation of enforcement and the latter's compatibility with higher-level law, notably fundamental rights and the ECD.[271] Art. 6 AVMSD thus creates a basis which, at least partially, counteracts the divergences in the na-

267 *Cole/Etteldorf*, in: Medienhandbuch Österreich 2019, p. 56, 60.

268 Cf. on this for example *Dittrich*, Social Networks and Populism in the EU – Four Things You Should Know.

269 For example the German Network Enforcement Act (cf. Chapter 2.4.4) or the French Loi visant à lutter contre les contenus haineux sur internet, http://www.assemblee-nationale.fr/15/ta/ta0310.asp.

270 For an overview on developments in Austria, Germany, Hungary, Italy, Poland and the United Kingdom cf. Art. 19 Free World Centre, Responding to 'hate speech': Comparative overview of six EU countries, available at https://www.Art.19.org/wp-content/uploads/2018/03/ECA-hate-speech-compilation-report_March-2018.pdf.

271 For the discussion on the German Network Enforcement Act cf. for example the documentation of the hearing of the Legal Committee of the German Bundestag on 15 May 2019, available at https://www.bundestag.de/dokumente/textarchiv/2019/kw20-pa-recht-netzwerkdurchsetzungsgesetz-636616.

tional legal systems of those Member States that decided to adopt separate legislation in that field.

Directive (EU) 2018/1808
Art. 6a
1. Member States shall take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. Such measures may include selecting the time of the broadcast, age verification tools or other technical measures. They shall be proportionate to the potential harm of the programme. The most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures.
2. Personal data of minors collected or otherwise generated by media service providers pursuant to paragraph 1 shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.
3. Member States shall ensure that media service providers provide sufficient information to viewers about content which may impair the physical, mental or moral development of minors. For this purpose, media service providers shall use a system describing the potentially harmful nature of the content of an audiovisual media service. For the implementation of this paragraph, Member States shall encourage the use of co-regulation as provided for in Art. 4a(1).
4. The Commission shall encourage media service providers to exchange best practices on co-regulatory codes of conduct. Member States and the Commission may foster self-regulation, for the purposes of this Art., through Union codes of conduct as referred to in Art. 4a(2).

With regard to the protection of minors in the media, former Art. 12 (previously for non-linear media services) and Art. 27 (previously for linear media services) were deleted and instead Art. 6a, as a provision relating to the protection of minors, which applies to all audiovisual media service providers, was standardised and simplified. It requires Member States to take appropriate measures to ensure that content of audiovisual media services which is detrimental to the development is made available only in such a way as to ensure that it cannot normally be heard or seen by minors. The choice of transmission time or means of age verification are cited as examples of implementation, and co-regulatory systems are advocated. With this formulation, television broadcasters are moving away from the complete prohibition of certain content that may seriously impair the development of minors, hitherto contained in Art. 27, towards a more openly formulated provision that covers both linear and non-linear offerings deal-

ing with pornography or gratuitous acts of violence in an equal manner.[272] However, as regards the possible measures, Art. 6a requires that the most harmful content (such as gratuitous violence and pornography) shall be subject to the strictest measures, including bans on broadcasting. On the other hand, there is no precise specification or balancing criteria to be applied. In addition, providers should make available sufficient information on content that may impair the physical, mental or moral development of minors, which will enable parents (but also regulators) to exercise better control. Personal data of minors must not be used for commercial purposes such as direct marketing or profiling – a provision which also takes into account the relevant considerations of the General Data Protection Regulation, which lays down that data of children enjoy special protection (e.g. Recital 38 of the GDPR).

For the cross-border distribution of online content, the provision regarding content which may impair the physical, mental or moral development of minors is particularly relevant. Each Member State must ensure (and in principle had to ensure under old law) that both linear and non-linear offers from VSPs (Art. 28b para. 1 lit. a) have no negative influence on the development of the personality of children and adolescents. However, the Directive does not define how this is to be ensured or what is to be understood as content that may impair minors' physical, mental or moral development. Numerous Member States have therefore developed different systems, in particular based on self-regulation and co-regulation, within which content and, in particular, age labels are reviewed.[273] In practice, when a specific content or offer is considered to impair the development of minors and should possibly be labelled or sanctioned (in the hardest case a ban), it is assessed on the basis of nationally established criteria (while there is a general statutory requirement such as under Art. 6a AVMSD). For example the Spanish Self-regulation Code for TV Content and Children, signed by several free-to-air linear providers, relies on several

272 In detail on the move away from the ban on pornography: *Ukrow*, Por-No Go im audiovisuellen Binnenmarkt?

273 Cf. in particular on self- and co-regulation systems: *Cappello (ed.)*, Self- and Co-regulation in the new AVMSD, IRIS Special 2019-2; on the legal situation under Directive 2010/13/EU see *Nikoltchev* (*ed.*), Protection of Minors and Audiovisual Content On-Demand, IRIS plus 2012; *Capello (ed.)*, The protection of minors in a converged media environment, IRIS plus 2015-1; and ERGA report on Protection of Minors in the Audiovisual Media Services: Trends & Practices, 2016, available at https://ec.europa.eu/digital-single-market/en/news/erga-report-protection-minors-converged-environment.

categories of impairing content (violence, sex, fear or anguish, drugs and toxic substances, discrimination, imitable behaviour and language)[274], and the German approved self-regulatory body for the telemedia sector defines impairing content as offers that are suitable for exerting a negative influence on the development of the personality of children and adolescents that contradicts the human image of the Basic Law whereby concretising this in its decisions[275]. While some content available on the Internet will certainly be considered as impairing the development of minors in all Member States (particularly in the area of pornography and violence) and is already stipulated by European fundamental rights, there will still be nuances of national differences.

Art. 9 of the AVMSD regulates advertising restrictions. The 2018 reform partially harmonised the legal framework for linear and non-linear services. The criteria under Art. 22, which until now only had to be complied with by television broadcasters in commercial communications for alcoholic beverages and which relate in particular to the prohibition of alcohol advertising aimed at minors and the positive presentation of alcohol consumption, now also apply to on-demand audiovisual media services. With regard to aspects relating to the protection of minors, the use of co-regulation and the promotion of self-regulation, in particular through codes of conduct, should be supported by the Member States in the advertising of alcoholic beverages. The same shall apply to inappropriate audiovisual commercial communication contained in or accompanying children's programs concerning food and beverages that contain nutrients or substances with a nutritional or physiological effect, in particular fat, trans-fatty acids, salt or sodium and sugar. This rule aims at effectively reducing the (positive) impact of such advertising on children and thus indirectly also the consumption of such foods and was therefore probably also connected with alarming reports of the World Health Organization on the worldwide increasing overweight among children in the run-up to the reform.[276]

The rules on the recognisability of advertising and the use of subliminal techniques have remained unchanged. Art. 1 para. 1 lit. c and g AVMSD, in particular, retains the rules which transpose the abovementioned con-

274 Cf. ERGA report on Protection of Minors in the Audiovisual Media Services, supra (fn. 273), p. 20.

275 For an overview of the decisions dealing with impairing content cf. https://www.fsm.de/de/downloads.

276 Report of the Commission on Ending Childhood Obesity (ECHO), 25.1.2016, available at https://www.who.int/end-childhood-obesity/en/.

siderations of human dignity, discrimination and protection of minors into the field of audiovisual commercial communication. Therefore, what has been mentioned applies – with some exceptions – accordingly: here, too, the national transpositions diverge[277]. With regard to alcoholic beverages, tobacco products and electronic cigarettes as well as prescription medicines, strong harmonisation across Europe exists as there is little or no room for manoeuvre in the Member States.

2.4.2.2.4. Supervision and Sanctions

Until the 2018 revision, the AVMSD contained no specific provisions on supervision[278] but merely required (or at least assumed) the existence of national regulatory authorities at certain provisions in the Directive.[279] Although the AVMSD, even after the 2018 reform, neither contains particular structural supervisory requirements nor explicitly requires Member States to set up an independent regulatory body or to define the terms of that independence, it is nevertheless noteworthy that Recital 94 and Art. 30 presume that the regulatory entities responsible for implementing the Directive's provisions are "independent regulatory bodies". This is an important step in the context of media regulation. The reluctance that nevertheless exists is certainly not least due to the fact that the EU only has limited competences in the field of cultural and media law (cf. already Chapter 2.3.2), that the (constitutional) traditions of the Member States have grown very differently, particularly in the media sector, and that, finally, in many Member States there are different supervisory structures (especially in federal systems) that would hardly be open to "standardisation" or harmonisation at European level. It is therefore the Member States that

277 For a detailed analysis cf. the study Defining a framework for the monitoring of advertising rules under the Audiovisual Media Services Directive, prepared for the European Commission by Ramboll Management Consulting and the Institute of European Media Law, available at https://ec.europa.eu/digital-single-market/en/news/audiovisual-and-media-services-directive-avmsd-study-advertising-rules.

278 Cf. on this ERGA's statement on the independence of NRAs in the audiovisual sector, ERGA(2014)03, October 2014, available at https://ec.europa.eu/digital-single-market/en/avmsd-audiovisual-regulators, and ERGA, Report on the independence of NRAs.

279 Cf. for example Art. 5 para. 1 lit. d, Art. 7 para. 2 and 3, Art. 28b para. 5 AVMSD.

must take the appropriate measures to ensure effective implementation of the Directive (in accordance with the duties imposed by the TFEU). They are free to choose the appropriate instruments according to their legal traditions and established structures, and, in particular, the form of their competent independent regulatory bodies in order to be able to carry out their work in implementing the AVMSD impartially and transparently.[280]

At national level, this can lead to very different forms of supervision, which can affect both structural issues (e.g. term of office of members of the supervision, allocation of funds, affiliation to state authorities or ministries, etc.) and competence issues (responsibility of different authorities for different areas of the AVMSD, allocation of enforcement powers, etc.).[281] This in turn can lead to legal uncertainties, especially in the regulation of cross-border online content (in conjunction with the country-of-origin principle on which the AVMSD is based), especially if the national regulatory authorities reach organisational or competence limits within the framework of the cooperation to which they are entitled under Art. 30 AVMSD.[282] For example, in a study carried out by the ERGA and published in 2015, five European regulatory authorities indicated that they did not have the necessary power to enforce their decisions autonomously and four national European regulatory authorities stated that in some cases the intervention of the Ministry/Government is needed for their decisions to take effect.[283] A further comparative study, in addition to the comprehensive study for the Commission in 2015[284], carried out by the EMR for the European Audiovisual Observatory, showed, for example, large differences in the selection, design and framework of sanctions: While the German media authority may take action against illegal telemedia offers, this is not possible for the Swedish media authority in this form; while the Latvian regulator has a sanction framework of 14,000 euros for the violation of content-related provisions, the German regulator can impose penalties of up to 500,000 euros; and while the Italian regulator can also take blocking

280 Cf. Recital 94 of Directive 2010/13/EU.

281 Cf. on this in detail: AVMS-RADAR, study prepared for the European Commission by the EMR and the University of Luxembourg, p. 40 et seq.

282 Cf. on this in general and for a comparative analysis of selected Member States: *Cappello (ed.)*, Media law enforcement without frontiers, IRIS Special 2018-2; and *Cappello* (*ed*.), The independence of media regulatory authorities in Europe, IRIS Special, IRIS Special 2019-1.

283 ERGA, Report on the independence of NRAs, pp. 51, 52.

284 AVMS-RADAR, study prepared for the European Commission by the EMR and the University of Luxembourg.

measures against platforms and websites, this is not possible in Sweden.[285] Moreover, self-regulation and co-regulation systems also have a different importance in the Member States, which is particularly evident in the area of advertising. While some regulators can take immediate action against providers themselves if they consider advertising to be inadmissible, regulators in other Member States have to maintain co-regulatory mechanisms in which it is foreseen that regulators have to first include opinions by self-regulatory institutions before being able to take action or in some cases are blocked from acting themselves.[286]

2.4.3. Data Protection and ePrivacy

With regard to data protection and the protection of privacy, the relevant secondary legislation determining the legal framework in the online environment is primarily the General Data Protection Regulation (GDPR)[287], which entered into force in May 2018, and the ePrivacy Directive[288]. Directive (EU) 2016/680[289] on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which repealed a Framework Decision[290] and was issued at the same time as the GDPR, applies to the exchange of personal data by national police and criminal justice authori-

285 *Cappello (ed.)*, Media law enforcement without frontiers, IRIS Special 2018-2, pp. 97 et seq.

286 Cf. *Capello (ed.)*, Self- and Co-regulation in the new AVMSD, IRIS Special 2019-2.

287 The provisions of the GDPR relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382,II. C.

288 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002 pp. 37–47.

289 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–131.

290 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, pp. 60–71.

ties. The Directive is intended to improve the exchange of personal data within the framework of law enforcement and to better protect the data of offenders, victims and witnesses by, inter alia, no longer requiring law enforcement authorities to apply different data protection rules depending on the origin of the personal data. Outside of the purposes mentioned in the Directive, however, the GDPR also applies to law enforcement authorities. Since the Directive essentially incorporates the principles laid down in the GDPR and plays a role in the context of this study only insofar as it concerns the criminal investigation and prosecution in the area of online-crimes, it is not supposed to be dealt with in the following in more detail.

2.4.3.1. Data Processing and the Media Privilege

Data processing activities are omnipresent on the Internet and the use of data is manifold. Electronic commerce requires personal data to process contracts concluded online, websites need personal data to ensure their operation and security[291], just as the way in which the business model of so-called intermediaries and other platforms depend on and are geared by the processing of personal data.[292] To cite one of the most famous examples, representing a number of business models in the digital economy, the social network Facebook stores and uses user data to offer personalised advertising. The frequently quoted sentence "Senator, we sell ads" by Facebook CEO Mark Zuckerberg at his hearing before the US Congress,[293] however, became famous against the rather sad background of the Cambridge Analytica scandal and the associated possibilities of influencing political elections.[294] This case shows not least the connection between data processing or power over data and the freedom of opinion and the freedom of the media directly connected with the formation of political opinion. Therefore,

291 Thus, when a website is called up, the service host regularly requests device data which, among other things, contains the IP address as a personal date in order to protect against unauthorised or damage-intended (e.g. DOS attacks) calls to the website, for example.

292 *Hans/Ukrow/Knapp/Cole*, (Neue) Geschäftsmodelle der Mediaagenturen.

293 Facebook chief executive Mark Zuckerberg appeared before the Senate's Commerce and Judiciary committees on 10 April 2019. For a transcription cf. https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/.

294 For an analysis cf., e.g., *Dutt/Deb/Ferrara*, "Senator, We Sell Ads": Analysis of the 2016 Russian Facebook Ads Campaign.

when, as in the context of this study, online content is mentioned, a distinction must first be made at this point between journalistic data processing and other (economic, technical, organisational and administrative) data processing activities against the background of the so-called media privilege.[295]

Pursuant to Art. 85 para. 1 GDPR, Member States are obliged to balance the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes, by means of legal provisions. If necessary, they should provide for derogations or exceptions from Chapters II to VII and Chapter IX in accordance with Art. 85 para. 2 GDPR. Against the background of media freedom, the GDPR thus recognises that the provisions on the protection of personal data cannot automatically apply to the processing of personal data for journalistic purposes, which is inevitably linked to the exercise of media freedom. These positions of the media protected by fundamental rights (in the form of freedom of reporting and research) and of the public (in the form of freedom to receive and disseminate information and ideas without official intervention and regardless of national borders) may, for example, require that the processing of personal data for journalistic purposes also is permitted outside the grounds set out in Art. 6 para. 1 GDPR or that rights of persons affected under Chapter III of the Regulation are restricted. This balancing act[296], i.e. the assessment of the extent to which the balancing of data subjects' interests and media/information interests requires modifications with regard to data protection provisions, is the responsibility of the Member States, which, however, have a wide margin of manoeuvre in this respect. In the field of journalistic data processing, European secondary law therefore does not provide a framework but leaves this largely to[297] the Member States. In order to do justice to the

295 Cf. *Cappello (ed.)*, Journalism and media privilege, IRIS Special 2017-2.

296 *Schiedermair*, in: Ehmann/Selmayr, Art. 85 GDPR para. 9.

297 By being bound by the fundamental rights of the Union, it also applies to the adoption of such legal provisions by the Member States that they must observe the rulings of the CJEU on the balancing of the right to informational self-determination with freedom of the media and freedom of information and that they must comply with the provisions of Art. 85 in the light of fundamental rights and the case-law of the ECJ; see, in particular, CJEU, judgements of 6.11.2003, C-101/01, *Criminal proceedings against Bodil Lindqvist*, para. 85 et seq.; of 16.12.2008, C-73/07, *Tietosuojavaltuutettu gegen Satakunnan Markkinapörssi Oy und Satamedia Oy*, para. 54 et seq.; of 13.5.2014, *Google Spain*, supra (fn. 79), para. 73 et seq.

tasks and functions of the media protected by fundamental rights, the concept of journalistic purposes must be interpreted broadly (Recital 153). With regard to the interpretation of the predecessor rule in Art. 9 of the DPD, the core of which was not touched within the GDPR either, the CJEU also confirmed this and clarified that exemptions should not only apply to media companies but to everyone who is active in journalism.[298] Therefore, Art. 85 GDPR can only be understood as meaning that the regulatory mandate to the national legislator does not only refer to the areas of "traditional press" and "traditional press activity". The GDPR therefore does not seek to seize activities whose goal exists in the passing on of information, opinions and conceptions to the public – as this was already planned by the definition in Recital 121 of an earlier draft of the Regulation[299].[300] This addresses the role of the media as an economic asset on the one hand and a cultural asset on the other.[301] The media privilege thus applies, for example, to private broadcasting when data collection is carried out for research purposes, e.g. for the production of articles as an intrinsic journalistic activity, but can also apply in individual cases to billing activities if these data are inseparably linked to a journalistic service (e.g. fee data of freelancers in particular in investigative journalism).[302] In the online context, the media privilege will therefore primarily affect the content itself, insofar as it also deals with personal data (e.g. within reports, news or documentaries and overall with regard to the perception of rights of depicted persons and actors), but not the mere accessibility of this content (e.g. via intermediaries such as search engines). In its landmark decision of 2014 in the *Google Spain* case, the CJEU stated that Directive 95/46/EC granted media privilege to Google Spain at the time: "Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circum-

298 CJEU, C-73/07, ibid., para. 56 and 58; cf. ECtHR, judgement of 27.6.2017, no. 931/13.

299 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Basic Regulation), COM(2012), 11 final, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

300 Cf. also *Cappello (ed.)*, Journalism and media privilege, IRIS Special 2017-2, pp. 13 et seq., on the scope of the media privilege as a whole.

301 Cf., e.g., *Von Rimscha/Siegert*, Medienökonomie pp. 227 et seq.

302 Cf. also in detail *Soppe*, in: ZUM 63(6), 2019, p. 467, 472, with further references.

stances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Art. 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights […] of Directive 95/46 against that operator but not against the publisher of the web page."[303] The purely economic operation of websites, media libraries, apps etc. is therefore generally subject to the provisions of European data protection law.

2.4.3.2. ePrivacy Directive and GDPR

In a further step the question about the relationship between the GDPR and the ePrivacy Directive is to be raised – in the ordered brevity. Art. 95 GDPR answers this question expressly in such a way that the GDPR "shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC". This means that there is a lex generalis-lex specialis relationship where the special provisions of ePrivacy Directive prevail over the general rules of the GDPR in areas which they specifically seek to regulate.[304] The European Data Protection Board (EDPB)[305] recently opted in this direction, holding in particular that the sanctions framework of the GDPR cannot be applied to cases that fall under the ePrivacy Directive.[306] The Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications net-

303 CJEU, *Google Spain v AEPD*, supra (fn. 79), para. 85.

304 However, that would not mean that generally further rules of the GDPR would be inapplicable. Thus, for example, Art. 6 does not contain any special defaults to the right of access, so that for this matter the provisions of the GDPR are still applicable.

305 EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

306 Cf. on this in detail *Etteldorf*, in: EDPL 5(2), 2019, p. 224, 226 et seq.

works and thus partly relies on the definitions in the Framework Directive for electronic communications networks and services.[307] Therefore, to fall under the scope of the ePrivacy Directive, services have to meet four criteria: (1) there is an electronic communications service[308]; (2) that service is offered over an electronic communications network[309], (3) both service and network are publicly available[310] and (4) service and network are offered in the EU.[311] Consequently only services consisting wholly or mainly in the conveyance of signals – as opposed to, e.g., the provision of content – fall within the scope of the ePrivacy Directive. However, convergence

307 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, pp. 33–50.

308 Art. 2 lit. d ePrivacy Directive specifies that "communication" means "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service" and excludes broadcasting services which may – in theory – reach an unlimited audience. The term "electronic communications service" is currently defined by Art. 2 lit. d Framework Directive as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services […] which do not consist wholly or mainly in the conveyance of signals on electronic communications networks".

309 An electronic communications network is defined in the Framework Directive as "transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed."

310 A service for the public is a service available to all members of the public on the same basis, and not only publicly owned services. Cf. EDPS, Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), available at https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf, p. 12; and Communication by the Commission to the European Parliament and the Council on the status and implementation of Directive 90/388/EEC on competition in the markets for telecommunications services, COM(95) 113 final, 04.04.1995, p. 14.

311 Cf. on the several conditions in detail *van Hoboken/Zuiderveen Borgesius*, in: JIPITEC 6(3), 2015, p. 198.

sometimes results in services that are very similar from a functional perspective but remain subject to different legal regimes depending on whether they are provided in form of an electronic communications service, an information society service or an audiovisual service.[312] Without going into detail on the scope of the ePrivacy Directive[313], it should be noted that – in the light of the objective of this Directive to ensure the protection of fundamental rights and freedoms of the public when they make use of electronic communication networks – at least some of its provisions also apply on providers of information technology networks (in particular Art. 5(3), 9 and 13).[314] Regarding the dissemination of content in the online environment this means that Art. 5 para. 3 and 13 of the ePrivacy Directive apply to website operators (e.g. for cookies) or other businesses (e.g. for direct marketing). For example, website operators have to obtain the (active)[315] consent of the user if they want to store (and subsequently use for e.g. personalised advertising) certain cookies on the end devices of website users, which in particular enables web tracking and is therefore essential for many advertising-based business models on the Internet. Consent is also required if advertisers want to address potential customers via electronic means of communication (e.g. e-mail) with direct marketing purposes.

This means that the distributors of online content as responsible parties (platform providers, website operators, etc.) must observe secondary legal requirements resulting from the implementation of the ePrivacy Directive in the Member States if they process personal data. However, like the AVMSD, the ePrivacy Directive contains no provisions on law enforcement, sanctions and the establishment of supervisory authorities. Rather, it is up to the Member States, who must ensure that the requirements are implemented, to decide how they are to be implemented. Similar to the AVMSD, this has led to a different implementation of the requirements[316],

312 *Dumortier/Kosta*, ePrivacy Directive: assessment of trans-position, effectiveness and compatibility with proposed Data Protection Regulation, p. 8.

313 For a detailed analysis cf. ibid.

314 Art. 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 9; Opinion 1/2008 on data protection issues related to search engines, WP148, p. 12.

315 Cf. in particular CJEU, judgement of 1.10.2019, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*.

316 Cf. National transposition measures communicated by the Member States, OJ L 201, 31.7.2002, pp. 37–47.

in particular with regard to the implementation of certain rules in general[317] or the responsibility of authorities to monitor the requirements. In Germany, Sweden and the UK, for example, there is a division of competences between the DPAs and the telecoms regulator in the area of electronic communications.[318] In addition, there is no forum under the ePrivacy Directive, such as the ERGA or EDPB, where an exchange could take place on the implementation and enforcement of the requirements of the Directive. Occasionally – and not established or prescribed by the Directive – coordination here can only take place via related instruments such as the EDPB or the Body of European Regulators for Electronic Communications (BEREC), although this is not expressly intended by the European legislator in the context of data processing within electronic communications networks. Especially in the online sector, which is the linchpin of the ePrivacy Directive, this is problematic due to the cross-border nature of online offerings. The same considerations as set out in point 2.4.2.2.4 apply.

The ePrivacy Directive is also currently undergoing a reform process. A proposed ePrivacy Regulation[319], introduced by the Commission in January 2017, should enter into force at the same time as the GDPR but is still – not least because of the controversial cookie regulation it contains – in the trilogue process. Therein particular rules are contained to the supervision, law enforcement and sanctioning of offences, referring to the corresponding regulations of the GDPR, so that in the future there will probably be a very broad synchronisation of these sets of rules.

Outside the regulatory framework of the ePrivacy Directive, the GDPR applies. Due to its character as a regulation, it is directly applicable in all Member States and has thus strongly harmonised the data protection laws throughout Europe. The Member States only have a few areas in which they have room for manoeuvre and which are expressly mentioned. The

317 In Germany, for example, there is no implementation of Art. 5 para. 3 of ePrivacy Directive according to the Positioning of the Conference of the Independent Data Protection Authorities of the Federal Government and the Länder on "Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018", available at https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf.

318 *Dumortier/Kosta*, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, pp. 33 et seq.

319 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

GDPR contains comprehensive provisions on principles, legality requirements and information obligations in connection with the processing of personal data. In addition, data subjects are granted comprehensive rights of control and access to processing operations. Although this certainly also plays an increased role in the online sector, that area will not be discussed in detail here, since questions of legality are ultimately questions of detail for the specific individual case.[320] However, the market place principle anchored in the GDPR, the comprehensive rules on supervision and sanctioning, and the system of cooperation within the EDPB are to be addressed in the following sections.

2.4.3.3. Market Location Principle

Under the conditions established by Art. 3 para. 2 lit. a and b GDPR, the scope of the GDPR extends to processing of personal data of data subjects located in the EU, without consideration of physical or operational structures of companies. With the introduction of this market location principle, the EU legislator thus extends the scope of application of European data protection law to data protection-relevant business activities of companies that do not have branches in the EU and would normally fall outside the territorial scope of application of EU law.[321] The aim was to ensure (Recital 23) that a natural person would not be deprived of his or her right to the protection of personal data simply because the processing is carried out by foreign providers. Thus, the GDPR takes its protection goal into account, which lies decisively in the protection of "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (Art. 1 para. 2 GDPR). The object of protection therefore determines the scope of application. However, it is not related to citizenship, residence or other types of legal status of the individual whose personal data are being processed, but only to the location of the

320 Although compliance with data protection law is rightly doubtful, especially on large online platforms such as Facebook, in view of recent rulings by the CJEU; cf. for example CJEU, judgement of 5.6.2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, regarding facebook fanpage; judgement of 29.7.2019, C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, concerning the facebook like button.

321 Cf. on the market location principle *Schantz*, in: NJW 26(69), 2016, p. 1841, 1842.

data subject in the Union.[322] The GDPR understands the Union thus as protected area, in which certain rights are guaranteed independently of Union citizenship.

The connecting factors for the market place principle and thus the applicability of GDPR are "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union" (Art. 3 para. 2 lit. a GDPR) or "the monitoring of their behaviour as far as their behaviour takes place within the Union" (Art. 3 para. 2 lit. b GDPR). Only in these cases, which are triggered by an independent and targeted action of the processing body, it is, according to the intention of the Union legislator, also in the interest of the enterprises to be subject to EU law.

In order to clarify in which situations goods or services within the meaning of Art. 3 para. 2 lit. a GDPR are directed towards a person, Recital 23 lists several criteria. According to that list, the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention. But factors such as whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union, which language or currency is used or if customers or users who are in the Union are mentioned can play a decisive role. In its Guidelines on the territorial scope[323], the EDPB mentions further criteria which could be taken into account like the use of a specific top-level-domain (".eu", ".de", etc.), the mention of dedicated addresses or phone numbers to be reached from an EU country, the international nature of an offer, the direction of advertisement or travel instructions for EU citizens. Furthermore, the EDPB considers that there needs to be a connection between the processing activity and the offering of good or service, but both direct and indirect connections are relevant and to be taken into account. It is notable that the aforementioned criteria show similarities to the criteria for assessing whether a broadcast by a media service provider established in another Member State is wholly or mostly directed towards the territory of another Member State in Recital 42 of the AVMSD (in the version of Directive 2010/13/EU).

322 Cf. Recital 14.

323 EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3), adopted on 16 November 2018, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf, p. 18.

Regarding the second alternative under Art. 3 para. 2 GDPR, Recital 24 clarifies that "[t]he processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects insofar as their behaviour takes place within the Union", and it names in particular "profiling" as activity the provision relies on. However, there are also other (mainly online) activities which could trigger the scope of Art. 3 para. 2 lit. b GDPR, such as behavioural advertisement, geo-localisation activities, fingerprinting, personalised diet and health analytics services, market surveys and other behavioural studies based on individual profiles.[324]

In order to fulfil the requirements under Art. 3 para. 2 GDPR, foreign providers must not only comply with the rules under the GDPR but also take into account the national regulations, which are the result of the discretion given to the Member States.[325] This extends the reach of the market location principle even further.

Beyond the applicability of Art. 3 para. 2 GDPR, however, action against EU foreign providers will continue to be based on requests for administrative assistance[326] or the exertion of influence on affiliated companies over which an original jurisdiction exists.[327]

---

324 See also EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3), supra (fn. 323), p. 18.

325 See also EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3), supra (fn. 323), p. 12.

326 Cf. on this for example the case of the data protection authority Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), described in 31th Activity report, 2009, chapter 7.4, printed papers 16/2439, available at https://www.datenschutzzentrum.de/tb/tb31/kap07.html#74. This case was about the website "rottenneighbor.com" where users could post (regularly negative) things about their neighbours by adding their location data. The German authorities approached the competent US Federal Trade Commission (FTC) and asked for remedy.

327 Cf. on this in detail already *Ukrow*, Zur Zuständigkeit der Landesmedienanstalten/KJM für ausländische Anbieter, p. 177.

2.4.3.4. Supervision and Sanctioning

Other than many other laws in the field of media and information-technical systems[328], the GDPR contains very extensive rules on supervision. Although the concrete establishment and structural design of the supervisory authorities is left to the Member States, it is determined to a greater or lesser extent by EU requirements. This was done considering that the "effective protection of personal data throughout the Union requires […] equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States" (Recital 11).

Points of contact which contain rules on the independent supervisory authorities are in principle[329] Art. 51 et seq. GDPR. Art. 51 of the GDPR requires each Member State to ensure that one or more independent authorities are responsible for monitoring the application of the Regulation in order to protect the fundamental rights and freedoms of natural persons with regard to processing and to facilitate the free movement of personal data within the Union. That complies with the goals mentioned in the GDPR (cf. Art. 1 GDPR). However, the focus is on the protection of fundamental rights and freedoms as a direct and actual purpose of the establishment of supervisory authorities. The supervisory authority must be in a position (factually and technically) to include fundamental-rights concerns in the monitoring of data processing operations of the responsible bodies subject to its supervision. Accordingly, Art. 53 para. 2 GDPR provides that *each member* of the supervisory authority must have the qualification, experience and expertise required for the fulfilment of its tasks and the exercise of its powers, in particular in the area of the protection of personal data, whereby the closer arrangement is left to the Member States (Art. 54 para. 1 lit. b GDPR). The term "members" here refers to the management level of the respective supervisory authority, which may vary depending on the implementation in the Member States.[330] They are the holders of the guaranteed independence and democratic legitimacy which must be en-

328 E.g. the AVMSD, the DSM Directive or the ECD.

329 According to Art. 85 para. 2 GDPR, Member States shall provide for exemptions or derogations from Chapter VI (independent supervisory authorities) in the field of the media privilege.

330 For this *Ziebarth*, in: Sydow, Art. 52 para. 21; in Germany, for example, the supervisory authorities of the Länder have only one member in this sense (Landesbeauftragte für den Datenschutz), while in Belgium a collegial body is appointed.

sured by the Member States when appointing them (under Art. 53 para. 1 of the GDPR, it must be ensured that each member of the supervisory authorities is appointed by means of a transparent procedure, whether by Parliament, the Government, the head of state or an independent body entrusted with the appointment under the law of the Member State).

Altogether, the independence of the supervisory authorities takes a special role in the context of the GDPR. Art. 52 GDPR lays down a number of requirements in order to guarantee the independence of the supervisory authorities, regulating in particular the freedom of the supervisory authorities from instructions from outside or inside, the personnel sovereignty and the necessity of the equipment with staff, technical and financial resources, premises and infrastructures. This also takes into account the fundamental rights requirements of Art. 8 para. 3 CFR. It should be emphasised at this point that adequate funding is intended to ensure independence, the establishment of a harmonised level of data protection and an effective protection of fundamental rights and is therefore of crucial importance.[331] Art. 53 GDPR supplements the provisions of Art. 52 GDPR, in particular to ensure the independence of members of supervisory authorities. For example, they must be appointed by an independent body through a transparent procedure, certain terms of office must be respected and there is some protection against unjustified dismissal.

The tasks and powers of the supervisory authorities are laid down in Art. 57 et seq. of the GDPR. Art. 57 GDPR, which lists various individual tasks, specifies the general monitoring activity already assigned to the supervisory authorities pursuant to Art. 51 GDPR, e.g. monitoring and enforcement of the ordinance (para. 1 lit. a) or the decision on complaints by persons concerned (para. 1 lit. f), on the one hand, but on the other hand also sets further requirements going beyond mere monitoring, e.g. raising public awareness (para. 1 lit. d) or the obligation to contribute to the activities of the EDPB (para. 1 lit. t). The supervisory authorities are therefore, on the one hand, "external supervisory bodies" in the sense of monitoring both without and (in the event of complaints) with regard to specific occasions; on the other hand, they perform[332] educational tasks comparable to media regulation authorities in the audiovisual sector. Art. 58 GDPR ensures that each supervisory authority has the necessary investigative, corrective and advisory powers at its disposal.

331 *Ziebarth*, in: Sydow, Art. 52 para. 40 et seq.
332 Cf. *Brink*, in: Wolff/Brink, § 38 BDSG para. 2.

In principle, the imposing of administrative fines for infringements of the GDPR is left to the Member States, whereby those fines shall be effective, proportionate and dissuasive (Art. 83 para. 1 GDPR). However, with regard to administrative fines that are imposed for infringements of the GDPR[333] by private entities[334], Art. 83 GDPR contains a comprehensive framework. On the one hand this is supposed to ensure that each supervisory authority (for the special cases of Denmark and Estonia cf. Recital 151) has the power to impose administrative fines and, on the other hand, to strengthen and harmonise administrative fines.[335]

2.4.3.5. Jurisdiction and Cooperation of Authorities

As regards the competence of the supervisory authorities, Art. 55 para. 1 GDPR provides that each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with the GDPR on the territory of its own Member State. This basically establishes the one-stop shop principle, which enables companies to address their concerns to the supervisory authority of the Member State in which they are established. The connection between Art. 3 para. 2 GDPR and the rules to the competence regarding the responsible supervisory authority also means that foreign service providers do not automatically benefit from the one-stop shop mechanism.[336] This principle applies only to processing entities established in the Union.[337]

In the case of cross-border situations that are the rule in the online environment, however, Art. 56 GDPR provides for rules deviating from the competence of the Member State of establishment. Nevertheless, Art. 56 does not apply to processing operations necessary to fulfil a legal obliga-

333 Regarding penalties for infringements of national rules, the Member States are enabled to lay down rules for (criminal and administrative) penalties, whereby the principle of *ne bis in idem*, as interpreted by the Court of Justice, should be taken into account; cf. Recital 149.

334 Regarding public authorities and bodies, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed; cf. Art. 83 para. 7 GDPR.

335 Cf. Recital 150.

336 See also EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3), adopted on 16 November 2018, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf, p. 12.

337 Cf. Art. 29 Working Party, WP244, 13 December 2016, Guidelines for identifying a controller or processor's lead supervisory authority.

tion to which the controller is subject (Art. 55 para. 2 in conjunction with Art. 6 para. 1 lit. c GDPR). This reflects the idea that Member States are empowered in this area to allow (relatively extensive) derogations from the GDPR, in particular to allow for the integration of national specificities in other sectors related to data protection law.

Art. 56 para. 1 GDPR regulates the competence of the lead supervisory authority in a way that the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor.

An exception to Art. 56 para. 1 is to be found under Art. 56 para. 2: By derogation from the one-stop shop principle, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State. As examples for processing activities concerning only processing carried out in a single Member State, Recital 127 names the processing of employees' personal data in the specific employment context of a Member State. In the cases referred to in Art. 56 para. 2 and 3, the supervisory authority shall observe a special procedure: In order to ensure the effective enforcement of a decision vis-à-vis the controller or processor, it shall inform the lead supervisory authority without delay about the matter, and the lead supervisory authority shall decide whether or not it will handle the case, by taking into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it (Recital 127). If the lead supervisory authority decides to handle the case, the procedure of cooperation between the supervisory authorities provided in Art. 60 GDPR shall apply, and the notifying supervisory authority should have the possibility to submit a draft decision, of which the lead supervisory authority should take utmost account when preparing its decision under the one-stop shop mechanism.

Art. 60 comprehensively regulates the cooperation procedure between the lead supervisory authority and the other supervisory authorities concerned in cases of cross-border data processing. The lead supervisory authority shall, inter alia, endeavour to reach consensus and provide other supervisory authorities involved with comprehensive information. The provision also includes procedural steps that give other supervisory authorities the possibility to make an objection against resolutions of the lead supervisory authority.

If a consensus ultimately cannot be reached, Art. 63 GDPR et seq. also provides for a consistency mechanism involving the EDPB. The EDPB was established under Art. 68 GDPR as a body of the Union with its own legal personality, composed of the head of the supervisory authority of each Member State[338]. Its main role is to ensure the consistent application of the GDPR throughout the European Economic Area – a task which is substantiated under Art. 70 para. 1 GDPR in more detail and in no less than 25 specific provisions. The EDPB will also be involved in advising the Commission, drawing up codes of conduct and certification mechanisms. In this role, the EDPB adopts, after extensive consultations, inter alia guidance in the form of guidelines, recommendations, best practices and opinions, thus clarifying the terms of the Regulation in order to provide a consistent interpretation of the rights and obligations of stakeholders. However, in cross-border cases where the cooperation procedure has led to no consensus, the EDPB has the power to rule on the matter by means of a binding decision, inter alia:

> "– where, in a case referred to in Art. 60 para. 4, a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation" (Art. 65 para. 1 lit. a);
> "– where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment" (Art. 65 para. 1 lit. b).

According to Art. 65 para. 2 GDPR, this decision shall be adopted within one month from the referral of the subject matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject matter. The decision shall further be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

338 Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Art. 63, Art. 51 para. 3 GDPR.

This gives the EDPB strong powers, compared to other authorities established at European level in the field of cross-border cooperation between supervisory authorities such as the ERGA, which, although linked to a complex and burdensome procedure, can lead to a final agreement in conflict cases.

2.4.4. Intellectual Property Rules

In the context of online content and related legal requirements, copyright plays an important role. Relevant legislative texts on EU level are the InfoSoc Directive of 2001[339], the Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Enforcement Directive)[340] and the DSM Directive[341], which is the legislative act that was recently adopted and amended the InfoSoc Directive and Directive 96/9/EC and has to be transposed by the Member States until 7 June 2021.

2.4.4.1. The InfoSoc and Enforcement Directives

The InfoSoc Directive, adopted on 22 May 2001, aims to harmonise key copyright and related rights issues in the EU and implements[342], inter alia, the 1996 WIPO Copyright Treaty. It contains a general regulatory framework, in particular with regard to reproduction and dissemination rights and most importantly concerning the communication to the public and making available to the public rights. These are property rights of the respective rights holders, who may permit or prohibit such acts in whole or in part and who are granted the right to bring an action for damages and/or a court order, among other things, with respect to infringements of their rights. In addition, the Directive contains a comprehensive list of copyright exceptions and limitations, which are exhaustively listed.

339 Directive 2001/29/EC, supra (fn. 15).
340 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, 30.4.2004, pp. 45–86.
341 Directive (EU) 2019/790, supra (fn. 16).
342 WIPO Copyright Treaty (WCT) – Joint Declarations, OJ L 89, 11.4.2000, pp. 8–14.

The Enforcement Directive of 2004 serves in particular to strengthen the rights of rights holders in order to ensure a high level of protection for intellectual property. It includes a wide range of enforcement instruments under private law, for example with regard to the preservation of evidence, information rights, interim measures or court orders.

2.4.4.2. The DSM Directive

The DSM Directive, which entered into force on 6 June 2019 after lengthy discussions, is based on, and supplements, the other relevant Directives with the aim of adapting copyright law in the EU to the requirements of the digital society. It includes rules on copyright contract law, text and data mining, ancillary copyright for press publishers, but also rules on the use of protected content by online services. In this latter area, the DSM Directive clearly departs from the principles of limited responsibility laid down in the ECD. It is especially interesting to consider in the legislative history of that Directive that there were numerous changes made to the text of this part of the Directive between the Commission's original proposal of 2016 and the finally adopted Directive of 2019. The core has remained, however, and that is bringing the possibility of direct platform liability more into focus when the DSM Directive will have been transposed. For this reason, the provisions of the relevant Art. 17 of the DSM Directive shall be examined in more detail in the context of this opinion.[343]

The rules contained in the DSM Directive on the use of protected content by online content-sharing service providers provide detailed guidelines on the liability of this type of platforms in the area of copyright.

The newly designed area of liability regulation within the framework of Art. 17 of the DSM Directive refers less to its own regime than to an explicit renunciation of liability privileges under the ECD in certain cases with regard to copyright infringing content on such online platforms. The DSM Directive currently in the process of being transposed in national law thus takes a step towards greater accountability of online platforms, albeit not on a cross-sectorial basis, as is the case for the ECD, but only in relation to certain areas of copyright law. The standard of liability and its enforcement in the cases covered by the DSM Directive shall subsequently be governed in particular by the standards laid down in the InfoSoc Directive

343 The provisions of the DSM Directive relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382, II. D.

and the Enforcement Directive. Because of the significant departure of the previously untouched liability regime of the ECD for platforms, it is worthwhile taking a brief look into the genesis of Art. 17.

The Commission's proposal on Art. 17 DSM Directive, at that time still Art. 13 of the proposal, which was not included in the final version of the DSM Directive, provided for a different wording, which could also be associated much more strongly with proactive obligations of the platform providers. Among other aspects, this wording referred to measures "such as the use of effective content recognition technologies"[344]. Recital 39 of the proposal claimed such technologies to be appropriate and proportionate measures to ensure protection of works. This wording fuelled the discussion about the future obligation of platform providers to establish so-called upload filters to ensure that copyright infringing material cannot be uploaded.[345] The argument was made that, to effectively recognise infringing content on a platform, a technology applied will have to examine the entirety of the content on the platform. This could, therefore, be seen in a way that Art. 13 of the proposal envisaged a general monitoring obligation.[346] This understanding of the proposal's wording was supported by the Commissions Impact Assessment on the modernisation of EU copyright rules[347], in which the Commission referred to "fingerprinting"[348] and

344 Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM/2016/0593 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0593:FIN.

345 Cf. on this in detail *Henrich*, Nach der Abstimmung ist (fast) vor der Umsetzung; *Kuczerawy*, EU Proposal for a Directive on Copyright in the Digital Single Market: Compatibility of Art. 13 with the EU Intermediary Liability Regime.

346 *Kuczerawy*, EU Proposal for a Directive on Copyright in the Digital Single Market: Compatibility of Art. 13 with the EU Intermediary Liability Regime, p. 10.

347 Commission staff working document, impact assessment, on the modernisation of EU copyright rules Accompanying the document Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market and Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, as of 14.9.2016, SWD(2016) 301 final, available at https://ec.europa.eu/digital-single-market/en/news/impact-assessment-modernisation-eu-copyright-rules, PART 3/3, p. 164.

348 Fingerprinting allows easily recognisable features of the content to be extracted and thus identified as unique features of that content. These features are then compared against a reference database.

"watermarking"[349] as two main types of content recognition technologies, in particular mentioning YouTube's Content ID system[350] as a prominent example for fingerprinting technologies.[351] However, the Commission's proposal was criticised for a number of factors. Concerns were raised in particular in light of the freedom of platforms to conduct a business, the freedom of expression of content creators and the right to protection of personal data (see Chapter 2.1.2). Above all, fears were voiced because of a possible collision with Art. 15 ECD, which prohibits Member States from imposing general obligations to monitor the information which service providers covered by the ECD transmit or store, and with the related case law of the CJEU (cf. on this in detail Chapter 3.3.7.3).[352] This led to an intensive search for a compromise in the course of the trilogue regarding former Art. 13:[353]

349 Watermarking is an invisible tattooing operation that only allows identifying tattooed copies. Digital watermarks are embedded into the content and make each copy of the content a unique copy.

350 The technological tool Content ID developed by Google allows the screening of visual and phonographic data of videos on YouTube and their automatic matching with other videos uploaded. In case a new video is uploaded on YouTube and a match is found against a "hash", the owner of the original content can decide whether content has to be blocked, content can be viewed freely and viewing statistics are gathered or content is being monetised (add advertisements); cf. https://support.google.com/youtube/answer/2797370?hl=en.

351 *Senftleben et al.*, in: European Intellectual Property Review 40(3), 2018, p. 149, 150 et seq.

352 See for example *Senftleben et al.*, in: European Intellectual Property Review 40(3), 2018, p. 149, 149 et seq.

353 Cf. the synopsis prepared by the Council, available at https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32019L0790.

COMMISSION'S PROPOSAL	Amendments of the Parliament[354]	General Approach of the Council[355]
1. Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate. The service providers shall provide rightholders with adequate information on the functioning and the deployment of the measures, as well as, when relevant, adequate reporting on the recognition and use of the works and other subject-matter.	1. **Without prejudice to Art. 3(1) and (2) of Directive 2001/29/EC, online content sharing** […] service providers **perform an act of communication** to the public […]. **They** shall **therefore conclude fair and appropriate licensing agreements with right holders.** 2. […] **Licensing agreements which are concluded by online content sharing** service providers **with right holders for the acts of communication referred to in paragraph 1, shall cover the liability for works uploaded by the users of such online content sharing services in line with the terms and conditions set out in the licensing agreement, provided that such users do not act for commercial purposes.** **2a. Member States shall provide that where right holders do not wish to conclude licensing agreements, online content sharing service providers and right holders shall cooperate in good faith in order to ensure that unauthorised protected works or other subject matter are not available on their services. Cooperation between online content service providers and right holders shall not lead to preventing the availability of non-infringing works or other protected subject matter, including those covered by an exception or limitation to copyright.**	1. *Member States shall provide that an* online content sharing service provider performs an act of communication to the public *or an act of making available to the public when it gives the public access to copyright protected works or other protected subject matter uploaded by its users. An* online content sharing service provider *shall obtain an authorisation from* the rightholders referred to in Art. 3(1) *and (2)* of Directive 2001/29/EC *in order to communicate or make available to the public works or other subject matter. Where no such authorisation has been obtained, the service provider shall prevent the availability on its service of those works and other subject-matter, including through the application of measures referred to in paragraph 4. This subparagraph shall apply without prejudice to exceptions and limitations provided for in Union law. Member States shall provide that when an authorisation has been obtained, including via a licensing agreement, by an online content sharing service provider, this authorisation shall also cover acts of uploading by the users of the service falling within Art. 3 of Directive 2001/29/EC when they are not acting on a commercial basis.* *[…]*

354 Amendments adopted by the European Parliament on 12 September 2018 on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market COM(2016)0593, available at http://www.europarl.europa.eu/doceo/document/TA-8-2018-0337_EN.html.

355 Document 9134/18 as of 25.5.2018, available at https://www.consilium.europa.eu/media/35373/st09134-en18.pdf.

		3. *When an* online content sharing service provider performs an act of communication to the public *or an act of making available to the public, it shall not be eligible for the exemption of liability provided for in Art. 14 of Directive 2000/31/EC for unauthorised acts of communication to the public and making available to the public, without prejudice to the possible application of Art. 14 of Directive 2000/31/EC to those services for purposes other than copyright relevant acts.* 4. *In the absence* of the authorisation referred to in the second subparagraph of paragraph 1, Member States shall provide that an online content sharing service provider *shall not be liable for acts of communication to the public or making available to the public within the meaning of this Art. when:* *(a) it demonstrates that it has made best efforts to prevent the availability of specific works or other subject matter by implementing effective and proportionate measures, in accordance with paragraph 5, to prevent the availability on its services of the specific works or other subject matter identified by rightholders and for which the rightholders have provided the service with relevant and necessary information for the application of these measures; and* *(b) upon notification by rightholders of works or other subject matter, it has acted expeditiously to remove or disable access to these works or other subject matter and it demonstrates that it has made its best efforts to prevent future availability through the measures referred to in point (a).*

The Parliament avoided an explicit mentioning of content recognition technologies but suggested nonetheless to oblige the service providers to ensure that unauthorised protected works are not available on their services. The Parliament addressed concerns regarding the collision with fundamental rights by a cooperation clause. The Council took a different ap-

proach. On the one hand, it implied a kind of notice and staydown mechanism in Art. 13 para. 4 lit. b) (Council Approach) requiring the service provider not only to remove the content in case of a notification but also to take additional measures to ensure that it is not subsequently reposted, either by the same user or by other users. On the other hand, it also required "best efforts" to prevent the availability of specific works or other subject matter by implementing effective and proportionate measures (Art. 13 para. 4 lit. a) of the Council Approach). However, such efforts would only be prescribed, according to the Council's approach, where the rights holders have provided the service with the relevant and necessary information for the application of these measures.

The differing positions led to a final compromise in Art. 17 of the DSM Directive which was no longer as strict as the Commission's original proposal but also included the approaches of Parliament and Council. Although Recital 66 DSM Directive now (only) states that "the obligations established in this Directive should not lead to Member States imposing a general monitoring obligation", the debate on content recognition technologies or other proactive measures is still relevant due to the relative general wording of Art. 17 DSM Directive, which continues to rely on appropriate and proportionate measures by demanding "best efforts" to ensure the unavailability of specific works. In this regard Art. 17 in its final version, which will be described in the following in more detail, still reflects a gradual shift in the perception of such platforms from being "mere conduits" to "active gate-keepers" of content uploaded and shared by users.[356]

Art. 17 DSM Directive, which regulates the liability of platforms, is applicable to "online content sharing service providers". These are platforms on which users can post large amounts of content and which make this available to the public, the main purpose of which must be to store and publish content uploaded by users.[357] The definition in Art. 2 para. 6 DSM Directive refers to the commercial nature of such a platform. Non-profit online encyclopaedias, science or education directories and open-source developer platforms are excluded. Moreover, providers of telecommunications or cloud services and online sales platforms are excluded, too. The storage and publication of content uploaded by users must be the "primary purpose" or "one of the primary purposes" of the platform concerned. The

356 In this regards also *Frosio/Mendis*, Monitoring and Filtering: European Reform or Global Trend?

357 DSM Directive, Recital 62.

Recitals narrow this down to those online services which play an important role on the market for online content by competing with other online content services, such as audio and video streaming services, for the same target groups. An assessment of this has to be made on a case-by-case basis.[358] A further partial restriction with regard to start-ups is made within the framework of Art. 17 para. 6 DSM Directive.

The starting point of the regulation is the clarification in Art. 17 para. 1 stipulating that the providers of such platforms themselves perform an act of communication to the public or an act of making available to the public within the meaning of the InfoSoc Directive (Art. 3) if the platform provides the public with access to works protected by copyright or other subject matters uploaded by its users. The service provider must therefore obtain the permission of the rights holders mentioned in Art. 3 para. 1 and 2 InfoSoc Directive for communication to the public or making publicly available.

Based on this finding, the essence of the new liability regime follows the conditions set by Art. 17 para. 3 DSM Directive. The liability privilege laid down in Art. 14 ECD therefore does not apply to the copyright-relevant actions of the users of the respective platform if they do not act commercially. In this respect, the Recitals[359] list those users whose activities are not for profit or whose activities on the platform do not generate significant revenues. In this case, platforms generally need to obtain the user rights granted by the respective rights holders in form of a licence agreement, or they are directly responsible for copyright infringements with the legal consequences provided for in the InfoSoc and Enforcement Directives.

However, the regulation offers a way out of direct liability. If, therefore, no licensing is possible for the activities of the users, the platform providers can resort to the envisaged alternative to the license agreements laid down in Art. 17 para. 4 in order to avoid direct liability. Art. 17 para. 4 DSM Directive provides for three conditions to be met cumulatively. Platforms must have made sufficient efforts to obtain authorisation from rights holders ("all efforts"), they must have made every effort to ensure that legally protected content is as inaccessible as possible ("in accordance with high industry standards of professional diligence"), and they must, as previously under Art. 14 of the ECD, remove content as soon as possible after becoming aware of it and prevent similar infringements of rights in respect of the work in the future (notice and takedown and staydown). As

358 DSM Directive, Recital 63.
359 DSM Directive, Recital 69.

mentioned, the reference to "content recognition techniques" as it appeared in the Commission's proposal for the DSM Directive was replaced. In this respect, Recital 66 speaks only of efforts to prevent the availability of unauthorised and other protected content recognised by the respective rights holders. In line with the principles of the ECD, the obligations laid down in the DSM Directive should not be induced to introduce a general monitoring obligation.

The requirement to prevent the availability of copyright protected content is also limited in two places. First, a proportionality clause in Art. 17 para. 5 determines the level of effort required, including the type, target group and size of the service and the works or other content uploaded by users, the availability of appropriate and effective means, and their cost to service providers. In turn, secondly, Art. 17 para. 6, according to which SMEs are exempted from obligations under certain conditions, must be cumulative. The exception applies in this respect to platforms that are less than three years old and have a turnover of less than EUR 10 million[360], which is why it can be referred to as a "startup-clause". These are now only obliged to seek authorisation and, as before, to remove any copyright infringing content after gaining knowledge. Those SMEs, which have more than 5 million monthly users, must at least prevent further uploads of this kind in the future. In addition, Art. 17 para. 9 contains further provisions according to which platforms are to provide their users with complaint mechanisms in the event that their content is incorrectly identified and treated as copyright infringement.

In addition, Art. 17 para. 7 clarifies that the justified use of copyright-protected content should remain protected within the framework of copyright barriers. In particular, with regard to the fundamental rights to freedom of expression and freedom of the arts enshrined in the CFR, a balance with intellectual property rights shall be found. To this end, the DSM Directive mentions quotations, criticisms, reviews, cartoons, parodies and persiflage as mandatory exceptions and restrictions. Service providers shall establish effective and expeditious complaint and redress procedures in the event of disputes concerning the blocking of access to and for removal of content in order to enable users to act within this framework.

By limiting the liability privileges established in the ECD and thus increasing the associated risk of direct liability to damages, the DSM Directive therefore not only places greater responsibility on platform providers in comparison with the previous liability framework but also goes one step

360 Calculated in accordance with Commission Recommendation 2003/361/EC.

further in comparison to other current regulations or regulatory undertakings, such as the German Network Enforcement Act (NetzDG)[361], which is already in force in Germany, or the Proposal of the European Commission for a Regulation for the Prevention of the Distribution of Terrorist Content Online[362], which do not rely on broad civil liability but on a system of sanctions. Under certain conditions, the functioning of the scheme de facto turns the fundamental principle of liability privilege under the ECD into a fundamental liability of intermediaries, albeit with exceptions.

2.4.5. Further Relevant Legislative Acts

2.4.5.1. Platform-to-Business Regulation

As part of its Communication Mid-Term Review on the implementation of the Digital Single Market Strategy[363], the Commission announced in May 2017 that it would take action to address unfair contract terms and unfair trading practices in relationships between platforms and companies. In particular, issues of dispute settlement, criteria for fair practices and transparency obligations should be clarified. The background was an inventory of platform-to-business trading practices, which indicated that some online platforms used trading practices that might discriminate against business users, for example by removing products or services from search results without adequate notice or even by favouring their own products or services.

The resulting Regulation on promoting fairness and transparency for business users of online intermediation services (Platform-to-Business Regulation, P2B Regulation)[364] came into force on 31 July 2019 and will

361 Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG) of 1 September 2017, BGBl. I, p. 3352.

362 COM/2018/640 final, supra (fn. 220).

363 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on the Mid-Term Review on the implementation of the Digital Single Market Strategy, A Connected Digital Single Market for All, COM(2017) 228 final.

364 Regulation (EU) 2019/1150 of the European Parliament and of the Council, of 20 June 2019, on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.7.2019, pp. 57–79.

be applicable as of 12 July 2020.[365] It is intended to achieve a better balance between platforms and businesses. The scope of the Regulation covers online brokerage services and online search engines which, through their respective platforms, offer goods or services to consumers located in the European Union, such as online e-commerce marketplaces, collaborative marketplaces, online services for software applications or online services for social media. Not included are, inter alia, peer-to-peer online intermediation services without the participation of commercial users or pure business-to-business online intermediation services which are not offered to consumers.

Core elements of the Regulation are, in particular, the obligation to set up an internal system for handling complaints from commercial users and information and transparency obligations. These include the disclosure of the main determining parameters for the ranking of an online intermediation service and the reasons for the relative weighting of these parameters. In addition, it must be broken down which data collected on the platform may also be used by the participating companies and which remain reserved for the provider of the platform.

With regard to enforcement, the Regulation refers to the Member States, which should adopt measures that are effective, proportionate and dissuasive and ensure the implementation of the Regulation. Reference is made to existing enforcement systems; the Member States are explicitly not obliged to set up new enforcement bodies.[366]

2.4.5.2. Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online

In order to prevent the spread of terrorist online content, the EU Internet Forum was first launched in December 2015 on the basis of an "European Agenda on Security" in order to combat the misuse of the Internet by terrorist groups. Voluntary measures and partnerships between Member States and hosting services were aimed at reducing the accessibility of online terrorist content, for example by setting up a hash database to ensure

365 The provisions of the P2B Regulation relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382, II. E.

366 P2B Regulation, Recital 46.

that content is permanently and irrevocably removed.[367] Most recently, the Forum participants agreed on an EU crisis protocol for a coordinated and rapid response to confine the viral spread of terrorist and extremist violence content.[368]

Independently of these discussions, in autumn 2018 the European Commission presented a draft Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (TERREG)[369] with the aim of improving the effectiveness of the current measures for the detection, identification and removal of terrorist content on online platforms.[370] The Commission followed an approach similar to that already established in Germany by the NetzDG. The proposed rules are primarily aimed at hosting service providers offering services within the Union, irrespective of their location or size, and there would not be a threshold or exception for Small and Medium Enterprises (SME).[371] In order to ensure the removal of illegal terrorist content, the draft Regulation provides for the possibility of a removal order, which may be issued in form of administrative or judicial decisions by a competent authority in a Member State. Hosting service providers can be obliged to remove content or deactivate access to such content within a very short time. In addition, providers may also need to take proactive measures to automatically detect and remove terrorist material. Furthermore, the draft includes safeguards to ensure the protection of fundamental rights. It mentions in Recital 5 that the newly (proposed) rules would leave untouched the liability privilege of the ECD.

More specifically, the draft Regulation contains due diligence, reporting and information obligations, the possibility of a removal order and, where appropriate, the obligation to take proactive measures. However, the draft Regulation does not contain a civil liability approach but instead refers to a system of sanctions. Illegal terrorist content as defined in the proposal is information used to incite and glorify terrorist offences and to invite people to contribute to these offences and content which contains instructions for the commission of terrorist offences or for promoting participation in

367 European Commission – Press release, EU Internet Forum: a major step forward in curbing terrorist content on the internet, Brussels, 8 December 2016.

368 A Europe that protects – EU Crisis Protocol: responding to terrorist content online, October 2019.

369 COM/2018/640 final, supra (fn. 220).

370 The provisions of the TERREG proposal relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382, II. F.

371 Explanatory Memorandum, 3.2 Impact Assessment.

terrorist groups[372], thus following the definition of terrorist offences in Directive (EU) 2017/541.[373]

The provision in Art. 6 of the draft Regulation, which states that hosting service providers may, where appropriate, be required to take "proactive measures", i.e. the use of automatic detection techniques, to protect their services against the dissemination of terrorist content, is subject to discussions in the legislative process and relevant with regard to the liability framework for hosting service providers. However, according to the draft Regulation, as mentioned above this should be done explicitly in accordance with the ECD. Thus, no (proactive) measure should in itself result in the service provider losing the right to the exclusion of liability granted under certain conditions in Art. 14 of the ECD. Nor should a decision by national authorities to implement proportionate and concrete proactive measures in principle result in Member States imposing a general monitoring obligation under Art. 15 para. 1 of the ECD.[374] According to Art. 6 para. 2 of the draft Regulation, proactive measures in this sense include, for example, automated tools to prevent the re-uploading of content that has previously been removed or blocked, or to immediately detect and block terrorist content. Such measures shall be effective and proportionate, taking into account the risks posed by the content concerned, the fundamental rights of users and the fundamental importance of the freedom of expression and information. In addition, Art. 9 of the draft Regulation provides for further safeguards with regard to the application and implementation of proactive measures.

As an enforcement instrument, Art. 17 of the draft Regulation sets out possible sanctions to be developed by the Member States, which should in principle be effective, proportionate and dissuasive. Specifically, the draft Regulation will address systematic violations of distance orders, under which Member States are to ensure that financial sanctions of up to 4% of the hosting service providers' worldwide annual revenue of the past financial year can be imposed. Sanctions, proactive measures and monitoring are in principle subject to the jurisdiction of the Member State in which the hosting service provider's principal place of business is located in ac-

372 Explanatory Memorandum, 1.3 Summary of the proposed Regulation.

373 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, pp. 6–21.

374 Explanatory Memorandum, 1.2 Consistency with existing EU legal framework in the policy area.

cordance with Art. 15 of the draft Regulation. Providers without a principal place of business in a Member State must appoint a legal representative whose location determines the jurisdiction.

2.5. EU Support, Coordination and Supplementary Measures

The area of support, coordination and supplementary measures at EU level includes various instruments which the European Commission uses either within the framework of its exercise of powers under Art. 2 para. 5 TFEU where the European Union lacks competence or to prepare legal acts for which it has competence under, for example, Art. 2 para. 2 TFEU. These (coordinating or preparatory) measures include, inter alia, the development of roadmaps showing how the Commission is planning to deal with an issue in the future, the setting up of working groups composed of experts and stakeholders and, finally, the development and issuing of recommendations which are adopted by the legislative bodies as non-binding instruments. In the area of regulation of online content, the Recommendations on the protection of minors and human dignity as well as two recent developments in the fields of hate speech and online disinformation are particularly relevant and will be presented below. Similar developments in the area of dealing with artificial intelligence will not be examined here, even though they play an important role in approaching challenges of the "digital world", as they do not directly relate to the area of content-related issues.

2.5.1. The Recommendations on the Protection of Minors and Human Dignity

First attempts to follow a horizontal approach across different types of content dissemination were made in 1998 with a Council Recommendation on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity (1998 Recommendation).[375] The 1998 Recom-

375 Council Recommendation of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effect-

mendation was based on the idea that the development of a competitive audiovisual and information service industry depends on the creation of a climate of confidence and hence on the protection of certain important general interests, such as the protection of minors and human dignity.[376] Therefore, the development of a common indicative framework at European level was considered being necessary, given the global character of the communication networks that needed to be dealt with. However, the importance of the subsidiary principle was stressed in light of the fact that the protection of minors is a culture-dependent issue for which the approach of each Member State is decisive.[377] Consequently, the 1998 Recommendation focussed on self-regulation by the industry and created guidelines for establishing a self-regulatory framework to protect minors on national level while addressing both Member States (to establish a (voluntary) national framework) as well as broadcasters and the respective industry (undertake research, promote cooperation, design codes of conduct, etc.). However, this framework was not to serve as replacement of or an alternative to the existing legal framework but rather to fulfil a supplementing function. The 1998 Recommendation was followed by several evaluation reports of the Commission concluding, inter alia, that it was applied quite heterogeneously and with differing degrees of commitment across the Member States, which was regarded to be possibly resulting from the cultural heterogeneity and varied development of the Internet use in the respective Member States.[378]

The 1998 Recommendation was further supplemented in 2006 by the Parliament and Council Recommendation on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry

---

ive level of protection of minors and human dignity, OJ L 270, 7.10.1998, pp. 48–55; cf. in detail: *Lievens*, Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments, pp. 103 et seq.

376 Cf. Recital 11 of 1998 Recommendation, supra (fn. 375).

377 Cf. Recital 16 and 18 of 1998 Recommendation, supra (fn. 375).

378 Cf., e.g., the 2001 Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity, COM/2001/0106 final, available at https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:52001DC0106.

(2006 Recommendation).[379] The output of the 2006 Recommendation can be split in three parts: firstly, guidelines for the Member States by establishing the necessary measures to ensure the protection of minors and human dignity, secondly, measures expected to be taken by the industry and, thirdly, activities that the Commission intended to tackle.[380]

With regard to the requirements to be satisfied by the Member States, it should be noted that, as already indicated in the Commission's second evaluation report from 2003[381] concerning the 1998 Recommendation, the 2006 Recommendation focuses more on aspects of co-regulation, although there is no concrete definition of that term. For instance, the Member States are encouraged to consider the introduction of measures in their domestic law or practice regarding the right of reply or equivalent remedies in relation to online media, to promote the take-up of technological developments (particularly regarding media literacy) in close cooperation with the parties concerned,[382] to promote a responsible attitude on the part of professionals, intermediaries and users of new communication media (in-

379 Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, OJ L 378, 27.12.2006, pp. 72–77; cf. on this in detail *Lievens*, Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments, pp. 112 et seq.

380 For example information campaigns, installation of a European freephone number to assist Internet users by directing them to available complaint mechanisms and information resources or to explore the possibility of supporting the establishment of a generic second level domain name reserved for monitored sites committed to respecting minors, etc. The provisions of the 2006 Recommendation relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382, III. A.

381 Second Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity, COM/2003/0776 final, available at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52003DC0776.

382 Annex II of the 2006 Recommendation outlines examples of possible actions naming: continuing education of teachers and trainers, in liaison with child protection associations, on using the Internet in the context of school education; introduction of specific Internet training aimed at children from a very early age, including sessions open to parents; an integrated educational approach forming part of school curricula and media literacy programmes, so as to provide information on using the Internet responsibly; organisation of national campaigns aimed at citizens, involving all communications media, to provide information on using the Internet responsibly; distribution of informa-

ter alia by drawing up a code of conduct in cooperation with professionals and regulatory authorities at national and Community level) and, finally, to promote measures to combat all illegal activities harmful to minors on the Internet and to make the Internet a much more secure medium, e.g. by adopting a quality label for service providers or by establishing appropriate means for the reporting of illegal and/or suspicious activities on the Internet.

Regarding the audiovisual and online information services industry, the 2006 Recommendation suggests developing positive measures for the benefit of minors, including initiatives to facilitate their wider access to audiovisual and online information services while avoiding potentially harmful content, for instance by means of filtering systems. Such measures, according to the 2006 Recommendation, could include harmonisation through cooperation between the regulatory, self-regulatory and co-regulatory bodies of the Member States and through the exchange of best practices, e.g. by using a system of common descriptive symbols or warning messages and by indicating the age category and/or which aspects of the content led to a certain age recommendation.[383] Furthermore, Member States were expected to develop measures to increase the use of content labelling systems for material distributed over the Internet and consider effective means of avoiding and combating discrimination.

The essence of the two Recommendations on the protection of minors and human dignity is threefold: Firstly, the need for special protection of minors and human dignity and the need for action in this respect was already recognised as early as 1998 with regard to the Internet and in particular by including the audiovisual and information society services industry in this process. Secondly, however, the European Commission saw the Member States as being responsible to take appropriate measures, inter alia, to take account of cultural specificities and different developments in

---

tion packs on possible risks of the Internet and the setting up of hotlines to which reports or complaints concerning harmful or illegal content could be addressed; adequate measures to establish or improve the performance of telephone hotlines.

383 Annex III of the 2006 Recommendation names examples of possible actions such as offering access to services specifically intended for children which are equipped with automatic filtering systems operated by access providers and mobile telephone operators; introducing incentives to provide a regularly updated description of the sites available; and posting banners on search engines drawing attention to the availability both of information about responsible use of the Internet and of telephone hotlines.

the digital environment of the respective state. Consequently, and because of their nature as non-binding acts, the Recommendations are weak in their wording (e.g. "encouraging" or "considering the introduction of measures") and merely provide a general framework, supplemented by proposals for more concrete examples of implementation. Thirdly, despite the non-binding and general wording, there are some aspects that are particularly emphasised for the creation of an appropriate regulatory environment: cooperation between the parties both in form of the states and the respective stakeholders, but also at international level and by involving the industry itself in the process.

2.5.2. The Actions Concerning the Tackling of Illegal Content Online

The cornerstone for countering illegal hate speech (online) was already laid with the 2008 Council Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law.[384] That Framework Decision provided for the approximation of laws and regulations of EU Member States on offences involving certain manifestations of racism and xenophobia. It was based on the obligation for Member States to introduce a criminal provision for certain serious manifestations of racism and xenophobia and make this type of crime punishable by effective, proportionate and dissuasive penalties. The Framework Decision detailed certain forms of conduct that fulfil the criteria to be regarded as criminal offences, inter alia, public incitement to violence or hatred directed against a group of persons or a member of such a group defined on the basis of race, colour, descent, religion or belief, or national or ethnic origin. The Member States had to ensure that such conduct is punishable by effective, proportionate and dissuasive penalties, which meant for a term of imprisonment of a maximum of at least one year, and, with regard to legal persons, the penalties had to consist of criminal or non-criminal fines and additionally other measures (e.g. exclusion from entitlement to public benefits or aid, temporary or permanent disqualification from practice or commercial activities, being placed under judicial supervision, etc.).

384 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, pp. 55–58.

However, at that time the Internet sector did not play a prominent role in the Framework Decision. Rather "the commission of an act […] by public dissemination or distribution of tracts, pictures or other material" (Art. 1 para. 1 lit. b Framework Decision) was covered in general. Yet, with the actual rise of hate speech in the online environment, this particular issue has become more and more prominent and has raised questions about how to combat it effectively.[385] Against that background, the Joint Statement issued by the extraordinary Justice and Home Affairs Council of 24 March 2016 on the terrorist attacks in Brussels underlined that "the Commission will intensify work with IT companies, notably in the EU Internet Forum, to counter terrorist propaganda and to develop by June 2016 a code of conduct against hate speech online"[386]. Subsequently, in May 2016, the Commission agreed with Facebook, Microsoft, Twitter and Google (YouTube) a "Code of conduct on countering illegal hate speech online" (in the following CCHSO)[387], which aimed to prevent and counter the spread of illegal hate speech online, to help users to notify illegal hate speech on social platforms and to improve the support by civil society as well as the coordination with national authorities.[388]

The CCHSO mainly addressed the problem that, although robust systems for the enforcement of criminal law sanctions against individual perpetrators of hate speech exist at national level, those systems need to be accompanied by effective measures in the online area, in particular with actions geared at ensuring that illegal hate speech online is expeditiously acted upon by online intermediaries and social media platforms, upon receipt of a valid notification, in an appropriate time-frame. Therefore, the signatories agreed, inter alia, to have in place clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content. In addition, they committed

385 Cf. for an overview and developments in CJEU case law *Belavusau*, in: Amsterdam Law Forum, 4(1), 2012, p. 20.

386 Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016, available at https://www.consilium.europa.eu/en/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/.

387 Available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en or http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

388 Cf. on the Code of Conduct in detail: *Quintel/Ullrich*, Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, Related Initiatives and Beyond.

to establishing rules or Community Guidelines clarifying that the promotion of incitement to violence and hateful conduct is prohibited on those platforms. Furthermore, they agreed to review the majority of users' notifications about alleged hate speech within 24 hours and to remove, if necessary, all those content assessed as being illegal. Further important points concerned the promise to further work on improving the feedback by the providers to users and being more transparent towards the general society by, inter alia, encouraging the provision of notices and flagging of content as described above. In this respect, the Commission sought to promote the adherence to the commitments set out in the CCHSO also to other relevant platforms and social media companies (in coordination with the Member States) and to assess the public commitments made on a regular basis.

In addition, in May 2016 the EU High-Level Group on combating racism, xenophobia and other forms of intolerance was set up to foster the further exchange and dissemination of best practices between national authorities and concrete discussions on how to fill existing gaps and better prevent and combat hate crime and hate speech. Since then, the High-Level Group serves also as platform for dedicated discussions on how to tackle specificities of particular forms of intolerance, also in light of the experience of civil society and communities. A sub-group on countering hate speech online deals with particular issues raised in the context of the CCHSO.

In the meantime, the Commission has issued the fourth evaluation on the EU Code of Conduct.[389] The Commission's assessment is generally positive: IT companies are now assessing 89% of the flagged content within 24 hours and 72% of the content deemed to be illegal hate speech is removed, compared to 40% and 28% respectively when the Code was first launched in 2016. Hence, from the perspective of the Commission, the CCHSO has been delivering continuous progress and contributed to the development of partnerships between civil society organisations, national authorities and signatory IT platforms on awareness raising and education activities. However, according to the Commission's assessment, the com-

389 European Commission, Factsheet February 2019, available at https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf.

panies need to further improve their feedback to the users notifying content and to provide more transparency on notices and removals.[390]

Despite the Commission's positive evaluation, it should not be forgotten in this context that the CCHSO is non-binding and that the signatories only voluntarily committed to the arrangements negotiated under the Code of Conduct. Withdrawal of this agreement is unilaterally possible at any time. This also applies to the data provided by the providers involved, which form the basis of the Commission's evaluation reports. For this it is not clear what data needs to be provided, and the access to the data can be unilaterally restricted at any time. It is therefore only an instrument of self-regulation with the corresponding disadvantages that this entails.[391] It has, however, made it possible to demand, with public visibility, compliance with these minimum standards and create greater awareness for the question of hate speech vis-à-vis the predominantly US-based IT companies[392], to which access on the part of the EU generally has been difficult. Correspondingly, the CCHSO is "aimed at guiding their own activities as well as sharing best practices with other Internet companies, platforms and social media operators".[393] The monitoring obligation of the European Commission as well as the (voluntary) obligation of the signatories to provide information and transparency add some elements which go in the direction of a co-regulatory mechanism, although there is no such obligation laid down in a binding legislative act. These mechanisms help to promote the effective implementation of the agreed measures. The CCHSO nonetheless does not contain any enforcement mechanisms or sanctions outside the publication of the assessment and progress by the Commission, which can only be regarded, to some extent, as constituting "moral sanctions" potentially affecting the public image of the concerned companies.

390 Cf. on this https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en.

391 Cf. on this Chapter 4.2.2.2 in detail.

392 Between 2018 and early 2019, *Instagram*, *Google+*, *Snapchat*, *Dailymotion* and *jeuxvideo.com* joined the Code of conduct.

393 Cf. on this also the announcement of the Code of Conduct on illegal online hate speech, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1937.

Finally, in the context of illegal content, the Communication on Tackling Illegal Content Online[394] published by the Commission in 2017 has to be taken into account as well, which then led to the Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online (Recommendation on Tackling Illegal Content Online)[395].

The Communication on Illegal Content Online lays down a set of guidelines and principles for online platforms (in particular hosting services provided by these platforms in the sense of Art. 14 of the ECD) aiming to facilitate and intensify the implementation of good practices for preventing, detecting, removing and disabling access to illegal content so as to ensure the effective removal of illegal content, increased transparency and the protection of fundamental rights online. It also aims at providing clarifications to platforms on their liability when they take proactive steps to detect, remove or disable access to illegal content (the so-called "Good Samaritan" actions). The Communication states that online platforms should systematically enhance their cooperation with competent authorities in the Member States, while the latter should ensure that courts are able to effectively react to illegal content online, as well as facilitate stronger (cross-border) cooperation between authorities. In that regard, online platforms and law enforcement or other competent authorities should appoint effective points of contact in the EU and, where appropriate, define digital interfaces to facilitate their interaction. Furthermore, the Commission encourages transparency, close cooperation between online platforms and trusted flaggers as well as the establishment of easily accessible and user-friendly mechanisms that allow their users to notify content considered to be illegal, automatic re-upload filters and counter-notice procedures.

However, what is particularly relevant for this study are the Commission's remarks in this context on the liability of hosting providers. In accordance with Art. 14 ECD, online platforms must take down illegal content

394 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, COM/2017/0555 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0555#footnote6.

395 Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177, available at https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32018H0334. The provisions of the Recommendation (EU) 2018/334 relevant in the context of this study are reprinted in the Online Annex, available at www.nomos-shop.de/44382, III. B.

expeditiously once they are made or become aware of its existence in order to be exempt from liability. The Commission is of the view that proactive measures taken by those online platforms to detect and remove illegal content which they host – including the use of automatic tools and tools meant to ensure that previously removed content is not re-uploaded – do not in and of themselves lead to a loss of the liability exemption. In particular, the taking of such measures need not imply that the online platform concerned plays an active role which would no longer allow it to benefit from that exemption. Whenever the taking of such measures leads to the online platform obtaining actual knowledge or awareness of illegal activities or illegal information, it needs to act expeditiously to remove or to disable access to the illegal information in question to satisfy the condition for the continued availability of that exemption.[396] Thus, according to the Communication, online platforms should do their utmost to proactively detect, identify and remove illegal content online; therefore it strongly encourages online platforms to use voluntary, proactive measures aimed at the detection and removal of illegal content and to step up cooperation and investment in, and use of, automatic detection technologies.

The subsequent Recommendation on Tackling Illegal Content Online, which takes up the descriptive approach from the Communication on Tackling Illegal Content Online in a somewhat streamlined form by transferring them in the form of more concrete rules, is particularly interesting with regard to two aspects: On the one hand, the first section contains a list of definitions that are strongly reminiscent of existing EU Directives. According to these definitions, for example, "hosting service provider" means "a provider of information society services consisting of the storage of information provided by the recipient of the service at his or her request, within the meaning of Art. 14 of Directive 2000/31/EC, irrespective of its place of establishment, which directs its activities to consumers residing in the Union", and "illegal content" means "any information which is not in compliance with Union law or the law of a Member State concerned". On the other hand, the Recommendation focusses on the cooperation between hosting providers and Member States (regarding, e.g., designated points of contact for matters relating to illegal content online and providing fast-track procedures to process notices submitted by competent authorities), (other) trusted flaggers (e.g. providing in a similar way fast-track procedures to process notices submitted by certified experts, publish-

396 Cf. Communication on Tackling Illegal Content Online, supra (fn. 394), para. 11.

ing clear and objective conditions for determining trusted flaggers) and other hosting service providers (e.g. by sharing experiences, technological solutions and best practices).

2.5.3. The Actions Concerning the Tackling of Online Disinformation

"Fake news" has gained increased attention in the media as well as in academic and political discussions, particularly in the context of the U.S. elections in 2016. The details about assumed targeted disinformation campaigns at that time have been dealt with elsewhere and therefore need not to be described in more detail in this study. However, they have been followed up by a number of political and regulatory activities at national and international level that require further consideration.[397]

On EU level, concrete measures tackling online disinformation started in 2017. A European Parliament resolution called on the European Commission to examine the current situation with regard to false reporting and to examine whether legislative measures could limit the dissemination of "fake news".[398] Subsequently, a High-Level Expert Group on Fake News and online disinformation (in the following HLEG), set up by the European Commission on 15 January 2018, consisting of 40 members (representatives of civil society, social media platforms and media organisations), began its work. The HLEG was to advise the Commission on the examination of that phenomenon, the roles and responsibilities of the relevant stakeholders and the international dimension, to take an inventory of the various positions and to issue recommendations. In March 2018, the HLEG handed over its report "A multi-dimensional approach to disinformation"[399] to the responsible Commissioner, in which the term "disinformation" was introduced for the first time ("The threat is disinformation, not 'fake news'"[400]), including forms of speech that fall outside illegal

397 In detail on this and the following as well as on developments on national level *Ukrow/Etteldorf*, „Fake News" als Rechtsproblem.

398 European Parliament resolution of 15 June 2017 on online platforms and the digital single market (2016/2276(INI)), available at http://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_EN.html?redirect, para. 36.

399 Report of the independent High level Group on fake news and online disinformation, A multi-dimensional approach to disinformation, published on 30.4.2018, available at https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1.

400 Ibid., p. 12.

forms of speech, notably defamation, hate speech or incitement to violence, but can nonetheless be harmful by transferring misleading or inaccurate information shared by people who do not recognise it as such. The report addressed all forms of false, inaccurate or misleading information designed, presented and promoted to intentionally cause public harm or for profit, and it recommended promoting media literacy to combat disinformation, developing tools to enable users and journalists to tackle disinformation, preserving the diversity and sustainability of European news media and continuing research on the impact of disinformation in Europe. In addition, the HLEG advocated a catalogue of principles to which online platforms and social networks should commit themselves.

On 9 November 2017, the Directorate-General for Communications Networks, Content and Technology presented its roadmap for the effective fight against "Fake News and online disinformation".[401] At the same time, a public consultation was launched. The roadmap stated that access to reliable information is a cornerstone of any functioning democracy and essential for the formation of the social (political) opinion. However, that opinion is increasingly threatened by the growing number of fake news and their distribution, especially on social media platforms. The Commission emphasises the danger posed by such false information aimed at undermining the functioning of political institutions or democratic decisions or by state-sponsored propaganda aimed at influencing elections or reducing confidence in democratic processes. While effective regulatory means supporting the fight against illegal content already exist at national and European level, there is a lack of such means for content that is not illegal per se but only "wrong".

Building on this assessment, the Commission published its communication "Tackling online disinformation: a European approach" in April 2018, which laid the foundations for further action.[402] The concept of disinformation coined by the HLEG was adopted but deviated from its definition, now being conceived as "false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm". The Commission considers

401 Communication on fake news and online misinformation, available at https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-5489364.

402 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, Tackling online disinformation: a European Approach, COM/2018/236 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236.

economic, technological, political and ideological circumstances to be the cause of the dissemination of disinformation. This includes, for example, the rise of platforms in the media sector, which in turn influences the more "traditional" media to the extent that they (must) seek new ways to monetarise their content, and the creation of new, or the manipulation of existing, technologies in the field of social networks, which enable or at least facilitate the dissemination of disinformation. Against this background, the Commission concludes that the fight against disinformation can and will only be successful in the long term if it is accompanied by a clear political will to strengthen collective resilience and support democratic efforts and European values. There is no single solution to this problem, given the many challenges arising from the complexity of the problem. There is, however, a need for action, and any political reaction should be comprehensive, continuously assess the phenomenon of disinformation and adapt the political instruments in the light of its development, according to the Commission.

In particular, the Commission identifies four main points which it considers to be essential for addressing problems in a solution-oriented way: Firstly, transparency must be created regarding the origin of information and the way in which it is produced, sponsored and disseminated. Secondly, diversity of information must be promoted to enable citizens to make informed choices, based on critical considerations. Thirdly, the credibility of information or credible information itself must be promoted. Fourthly, the development of integrated and long-term solutions requires awareness raising, promotion of media literacy, broad stakeholder involvement and cooperation between public authorities, online platforms, advertisers, journalists and media groups.

Finally, after this long process of evaluations, representatives of online platforms, leading social networks[403], advertisers and advertising industry agreed together with the Commission on a self-regulatory Code of Practice to address the spread of online disinformation and fake news (in the following CPD).[404] The CPD set a wide range of commitments, from transparency in political advertising to the closure of fake accounts and the demonetisation of purveyors of disinformation within the framework of ex-

403 The companies involved were *Facebook*, *Google*, *Twitter* and *Mozilla*.

404 EU Code of Practice on Disinformation, available at https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

isting EU legislation and Member States law.[405] The CPD stated, in particular, that the ECD and particularly Art. 12–15 shall be considered in the context of any obligation of the Code which targets mere conduits, caching providers or hosting providers such as providers of network, search engines, browsers, online blogging platforms, online forums, video-sharing platforms or social media. It includes commitments regarding the scrutiny of ad placements, political advertising and issue-based advertising, the integrity of services and the empowering of both consumers and the research community. In this regard the CPD is even more detailed in comparison with the aforementioned CCHSO. Regarding the monitoring of effectiveness, the signatories commit to write a (further detailed) annual report of their work to counter disinformation. That report shall be issued in form of a publicly available report reviewable by a third party.

Although the CPD is, like the Code of Conduct, non-binding, it is more detailed in content than the CCHSO and contains stronger formulations and more concrete requirements. The mechanisms of co-regulation are also less pronounced here. Signatories commit to select an objective third party organisation (besides the Commission) to review the annual self-assessment reports submitted by the signatories and to evaluate the level of progress made against their commitments. It needs to be underlined that also in this respect neither the actual degree of commitment nor the possibility to monitor it is very clear. Both the compliance with the CPD requirements and the making available of the corresponding data by the companies in order for third parties to review the measures are merely voluntary and cannot be demanded by an authority or sanctioned in case of non-availability or non-compliance. The evaluation problems resulting from this have already been expressed by the ERGA in its report of the activities carried out to assist the Commission in the intermediate monitoring of the Code of Practice on Disinformation as follows: "The platforms were not in a position to meet a request from ERGA to provide access to the overall database of advertising, even on a limited basis, during

405 In particular the EU Charter of Fundamental Rights, the European Convention on Human Rights, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market, Directive 2006/114/EC concerning misleading and comparative advertising and the case law of the CJEU and ECHR on the proportionality of measures designed to limit access to and circulation of harmful content.

the monitoring period. This was a significant constraint on the monitoring process and emerging conclusions."[406]

The Code includes an annex identifying best practices that signatories commit to apply to implement the Code's provisions. These best practices bring together the approaches of stakeholders, as laid down in the various stakeholder policies, in a general approach. In the area of advertising policies, the stakeholders endeavour to tackle disinformation by pursuing "follow the money" approaches[407] and prevent bad actors from receiving remuneration.[408] In the field of political advertising, online platforms are developing solutions to increase transparency of such advertising and enable consumers to understand why they are seeing those ads. Platforms announced to develop tools so that civil society is able to better understand the political online advertising ecosystem.[409] Platforms seek to safeguard service integrity by applying policies which limit the abuse of their service by inauthentic users, for example by policies restricting impersonation on YouTube.[410] Finally platforms announced to provide users with information, tools and support to empower consumers in their online experience (including also redress and reporting systems) and committed to support the research community by providing data[411] and creating own research

406 ERGA, Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation, June 2019, available at http://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf.

407 The follow-the-money approach in general is aiming to cut the revenue resulting from right infringements. The Commission has committed in its Communication on a strategy for the Digital Single Market to adopting a "follow the money" approach aiming to cut the revenue flows that drive commercial-scale IPR infringers into their activities. The approach seeks to create a Memorandum of Understanding where signatories put in place mechanisms to minimise the placing of online advertising on websites which infringe intellectual property rights.

408 Facebook, e.g., by reducing the distribution of economic incentives for false news and inauthentic content like clickbait and by informing people by giving them more context on the posts they see; cf. Facebook false news policy, available at https://www.facebook.com/communitystandards/false_news.

409 E.g. Googles' control systems for consumers to determine what advertisements they see; cf. Google ad settings, available at https://support.google.com/ads/answer/2662856?hl=en-AU.

410 Cf. YouTube Policy on impersonation, available at https://support.google.com/youtube/answer/2801947?hl=en-GB.

411 For example Facebook's "Initiative to Help Scholars Assess Social Media's Impact on Elections"; more information at https://newsroom.fb.com/news/2018/04/new-elections-initiative/.

initiatives. These aimed-at best practices should also provide solutions and ideas for smaller companies to combat disinformation.

Concerning the Code of Conduct, as a last point the action plan against disinformation that the Commission presented on 5 December 2018 should be mentioned.[412] In that plan, the Commission and the High Representative for Foreign Affairs and Security Policy propose concrete measures to combat disinformation. These include the establishment of an early warning system, the close monitoring of the implementation of the Code of Conduct and an increase in funding for those purposes. Moreover, the exchange of data between Member States is to be facilitated and additional funding for media literacy projects is to be made available.

412 European Commission contribution to the European Council Action Plan against Disinformation, 5.12.2018, available at https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.