RICKERT.LAW

Rickert Rechtsanwaltsgesellschaft mbH· Colmantstraße 15· 53115 Bonn

Dresden Higher Regional Court
Schloßplatz 1
01067 Dresden

per beA

Your sign:		Clerk:	RA Thomas Rickert
Our sign:	RIC-23/149/06/TR	Email:	kanzlei@rickert.law

Bonn, the 07.06.2023

In the litigation
Sony Music Entertainment Germany GmbH ./.
Quad9 Foundation
14 U 503/23

We thank you for the extension of time granted. In the following, the appeal filed in the name of the defendant and appellant against the judgment of the Regional Court of Leipzig, File No. 05 O 807/22 of 01.03.2023 with the following motions is substantiated:

It will be requested,

> to dismiss the action, amending the judgment of the Leipzig Regional Court of March 1, 2023, Case No. 05 O 807/22.

As a precautionary measure, in the event that we are unsuccessful, we request that the appeal be allowed.

Rickert Law Firm Ltd.

Lawyers
Thomas Rickert[1]
Patrick Jardin[2]
Carsten Toß[2]
Roman Wagner[4]
Matthias Bendixen[3]
Nicolas Golliart[3]
Lena Aquarius[3]
Sandra Schulte, LL.M.[3]
Theresa Müller-Sevindik[3]

Law firm
Colmant Street 15
53115 Bonn
Tel.: +49.228.74 898.0
Fax: +49.228.74 898.66
www.rickert.law

HRB 9269
AG Bonn

Business account
Commerzbank AG
IBAN: DE81 3804 0007 0241 4480 00
BIC: COBADEFF380

Deutsche Bank AG
IBAN: DE20 3807 0059 0053 1012 00
BIC: DEUTDEDK380

Escrow account
Commerzbank AG
IBAN: DE55 3804 0007 0241 4480 80
BIC: COBADEFF380

[1]Managing Partner
[2]Senior Associate Partner
[3]Associate Partner
[4]Of Counsel

A. Preliminary remark

The Leipzig Regional Court erred in law in classifying the defendant's service because it assumes that the resolution of domain names into IP addresses can give rise to perpetrator liability for copyright-infringing content. The Leipzig Regional Court errs in applying principles of law that the European Court of Justice and the German Federal Court of Justice have developed for certain categories of hosting providers. However, hosting providers or platforms through which content is made available for retrieval via the Internet are fundamentally different in terms of their technical functionality and also the provider's ability to influence content posted by customers to operate a DNS resolver.

A DNS resolver is a software module operated by the defendant that acts as a mere technical interface between users who make DNS requests and DNS servers that have information about which IP address is assigned to the requested domain. Through this interface, users cannot upload content or select whether and, if so, with whom they want to share content, but this was a requirement in the cases decided by the ECJ (see ECJ, Judgment of 22 June 2021, Cases C682/18 and C683/18, para. 74 - YouTube/Cyando).

Furthermore, no links/hyperlinks can be uploaded that provide access to content. Only those providers or platforms that enable uploading as well as the management of the uploaded content, or publish publish download links on the Internet that provide access to the content on the platform can perform an "*act of reproduction"* because, without the consent of the rightholders, they can grant other Internet users access via these platforms to protected works that those other Internet users would not have been able to access had the first-mentioned users not taken action (see ECJ, Judgment of 22 June 2021, Cases C682/18 -and C683/18-, para. 75 - YouTube/Cyando).

A corresponding subsumption for the DNS resolver service of the defendant is not possible to begin with and is also not made by the Leipzig Regional Court.

Finally, the statements of the Regional Court are illogical and contradictory when, on the one hand, it assumes a perpetrative act of communication to the public and thus a central role of the service provider (Judgment, p. 11), but at the same time denies the defendant the status of a service provider and thus the liability privilege under Section 8 (1) sentence 2 of the German Telemedia Act (TMG) due to a lack of sufficient possibility of influence (Judgment, p. 10).

A short video presentation available at the URL https://www.youtube.com/watch?v=HdC7Dy7xLzU illustrates the neutral and automatic operation of a DNS resolver. It can be seen that no storage or holding of content is performed by a DNS resolver.

Since the judgment shows serious errors in the subsumption of the defendant's service, completely disregards legal regulations that are beneficial to the defendant, and does not sufficiently appreciate the defendant's submissions from the I Instance, the judgment is set for review by the Court of Appeal in its entirety.

B. Justification

The judgment of the Leipzig Regional Court is based on an incorrect application of the law under sections 513 (1) and 546 of the German Code of Civil Procedure (ZPO). The plaintiff has no claims against the defendant for injunctive relief or blocking.

I. Indefinite omission tenor

The operative part of the judgment of the Leipzig Regional Court is not sufficiently specific, as it contains the wording "and/or the further domain(s)" (judgment, p. 2). Taking into account the BGH judgment "DNS-Sperre" (BGH, judgment of October 13, 2022 - I ZR 111/21, GRUR 2022, 1812), an application or operative part is unspecific if no blocking of a specific domain is requested (duplicate of January 30, 2023, p. 18; BGH, loc. cit. para. 72f.).

The Regional Court is under the mistaken assumption that the plaintiff's most recently filed request satisfies the definiteness requirement of Section 253 (2) no. 2 of the German Code of Civil Procedure. This contradicts the district court's own legal statements (judgment, p. 9), according to which a "concrete domain" must be named in accordance with the DNS blocking decision of the Federal Court of Justice (BGH, loc. cit.).

II. no active legitimation

The Regional Court errs in law in assuming that the plaintiff has the right to sue. The District Court merely based the plaintiff's right to bring an action on the existence of a presumption of entitlement, which is not relevant here, without examining the actual prerequisites.

1. no ancillary copyrights / no sufficient rights of use

The Regional Court assumes that the plaintiff has the right to bring an action (judgment, p. 10), because the plaintiff is designated as the holder of exclusive rights of use on copies of the sound carrier containing the music album in dispute. At the same time, however, the plaintiff is also the owner of the ancillary copyrights of the sound carrier manufacturer (judgment, p. 10).

Original and acquired ownership of rights are different situations which are logically mutually exclusive. Thus, on the one hand, it is claimed that the requirements for the creation of the respective property right were fulfilled by the owner himself and, on the other hand, that a third party fulfilled these requirements and that the property right thus created was subsequently transferred or licensed by concluding a contract. Consequently, the different findings of the Leipzig Regional Court do not make sense, since the holder of ancillary copyrights already owns the exclusive rights, and consequently no exclusive rights of use need to be granted.

It is not clear from a P-notice whether the notified party is the manufacturer, the legal successor or the holder of exclusive rights of use. Consequently, the P-notice can be considered for all three functions. The presumption under Section 10 (3) UrhG cannot be used to infer a transfer of full rights. The Federal Court of Justice (BGH, judgment of June 2, 2022 - I ZR 140/15, marginal no. 40 YouTube II) has stated that the P-notice can also merely indicate that only

certain exclusive rights of use have been granted to the company (duplicate of January 30, 2023, p. 19).

The defendant already stated in its statement of defense (statement of defense dated July 29, 2022, p. 25) that the P-notice cannot be used to infer ownership of the rights to the disputed music album, particularly since the issue in this case is not the physical distribution of the sound carrier, but an alleged infringement of the right to make the disputed sound recordings available to the public.

2. No infringement of the right of public access by hyperlinks on the disputed website

The Regional Court justifies the perpetrator's liability of the defendant with an infringement of the right of making available to the public pursuant to §§ 15, 19a, 85 UrhG (judgment, p. 11). It errs in law in assuming that the publication of hyperlinks on the website in dispute infringed the plaintiff's rights as a producer of sound recordings pursuant to § 85 UrhG. This is also relevant to the decision, since the district court assumes that the defendant could have recognized with "a look at the character of the page" that there were obviously exclusively illegal offers on the website in dispute (judgment, p. 12).

However, the phonogram producer's right pursuant to Section 85 UrhG does not grant the phonogram producer any right of communication to the public - with the exception of the right of making available to the public. Holders of ancillary copyrights cannot invoke the right of communication to the public pursuant to Section 15 UrhG in conjunction with Art. 3 (1) InfoSoc Directive. Article 3 (1) of the InfoSoc Directive because they do not have a comprehensive right of communication to the public (Schulze in: Dreier/Schulze, Urheberrechtsgesetz, 7th ed. 2022, Section 85 no. 38).

The District Court fails to recognize that the publication of hyperlinks on the website in question does not affect the right of public access. The setting of hyperlinks only constitutes making available to the public pursuant to Section 19a UrhG if the subject matter of the protection is in the sphere of the party providing the link. (BGH, judgment of September 21, 2017 - I ZR 11/16, marginal no. 19, GRUR 2018, 178 - Vorschaubilder III). The operators of the website in dispute can therefore not be accused of making the material publicly available, as the sound recordings were located on the servers of a third party and thus outside their sphere of access. The plaintiff cannot rely on a possible infringement of the right of communication to the public, on which the District Court refers to the case law of the ECJ (judgment, p. 11), since the right to produce sound recordings asserted by it does not include this right.

Those who make a fixed performance available for download themselves make it publicly accessible, since only the members of the public determine whether, when and where they access it. Consequently, the decision that the related subject matter is made available to the visitors of the platform lies exclusively with the platform users or the operators of these platform users (cf. Grünberger, Michael: Die Entwicklung des Urheberrechts im Jahr 2022; ZUM 2023, 309, 332).

> *"It must therefore be held, first, that the users of the platforms at issue in the main proceedings perform an 'act of communication' within the meaning of the case-law cited in paragraph 68 of the present judgment when, without the consent of the rightholders,*

they give other internet users access, via those platforms, to protected works which, had the first-mentioned users not acted, those other internet users would not have been able to access. Second, only if those users make the uploaded content available to the "public" within the meaning of the case law cited in para. 69 of the present judgment by sharing that content with every Internet user on the YouTube platform or by publishing on the Internet the download links that provide access to the content on the Uploaded platform, is there a possibility that those users and, consequently, the operator of the platform through which that access is made available, will engage in "communication to the public" within the meaning of Article 3(1) of the Copyright Directive. (ECJ, Judgment of 22 June 2021, Cases C-682/18 and C-683/18, para. 75 - YouTube/Cyando).

Assuming that the defendant would make a public reproduction of the hyperlinks by resolving the domains into an IP address, the plaintiff could not derive any entitlement from this. Consequently, the District Court assumed the plaintiff's right to bring an action on the basis of an incorrect presumption.

III. No liability of the defendant for infringements on the disputed website

The plaintiff cannot assert claims for injunctive relief, damages and removal against the defendant, as the defendant's service is privileged against liability pursuant to Section 8 (1) sentence 2 TMG.

1. the Defendant is a service provider pursuant to Section 2 No. 1 TMG

The Regional Court assumes that the liability privilege pursuant to Section 8 (1) sentence 2 of the German Telemedia Act (TMG) does not apply because it wrongly assumes that the defendant is not a service provider within the meaning of Section 2 no. 1 of the TMG and states (judgment, p. 10):

"However, this does not apply to a DNS resolver. The term "service provider" is to be defined functionally (Hamburg Regional Court, decision dated May 12, 2021, file no. 310 O 99/21, Annex K 1). The service provider must enable the dissemination or storage of information through its instructions or its power over computers and communication channels and must appear to the outside world as the provider of services. The Admin-C, for example, is not a service provider because it only facilitates the processing of domain registration, but neither provides information nor arranges access to it. The registrar likewise does not provide users with information or mediate access to the use of telemedia, but merely handles the administrative processing of domain registration by providing the registry with the data required to register the domain. In particular, it is not an access intermediary within the meaning of Section 8 of the German Telemedia Act (TMG), because it neither provides access to a network nor passes on information (BGH, judgment of October 15, 2020-tzR13/19, GRUR 2021, 53.64 marginal no. 15_17 with further references). The same applies in any case to the case of the DNS resolver at issue here (LG Hamburg, loc. cit.)."

The district court here uses the correct definition of the Federal Court of Justice as a basis, but thereafter omits any subsumption.

The defendant is a service provider within the meaning of the German Telemedia Act (TMG) because, pursuant to § 2 no. 1 alt. 2 TMG, it provides access to the use of telemedia. The defendant's service is an essential component of the provision of access to telemedia (MMR 2023, 378, 381), namely the retrieval of web pages after calling up a domain (statement of defense of July 29, 2022, p. 26f.). Unlike the domain registrar, the defendant's service is itself involved in the technical provision of access and is therefore also to be classified as a service provider under the case law of the Federal Court of Justice (BGH, judgment of October 15, 2020 - I ZR 13/19, para. 17). The "connection" to the requested domain desired by the inquirer is made automatically by entering the URL in the browser window. The DNS resolver, as an essential interface in the DNS, converts the host name contained in a URL into an IP address so that the requestor can retrieve the content of the website that can be reached via the domain. Without the DNS resolver, no assignment of the domain to the IP address would take place, so that no access to the desired telemedium would be possible in this way. The fact that the defendant does not directly open access to the website in question is irrelevant, since the wording of "mediation" also suggests indirect opening of access, i.e. a broad understanding of the term (statement of defense dated July 29, 2022, p. 26f.). In addition, "direct access" is only possible by means of the IP address. However, if a domain is called up, it is a technical necessity that first its resolution is made via the DNS and in a second step the web server is called up.

This interpretation also follows from the clear requirements of Union law (MMR 2023, 378, 380). In Art. 2 lit. b of the E-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council, hereinafter: ECRL), "service provider" is defined as any natural or legal person offering an information society service. The term "information society service" is legally defined in Article 1(1)(b) of Directive (EU) 2015/1535 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient". This applies to the service of the defendant (MMR 2023, 378, 381). The fact that the service is free of charge is irrelevant for this purpose (ECJ, judgment of September 15, 2016, Case C-484/14 - McFadden, paras. 41, 43).

According to the wording of Section 2 No. 1 of the German Telemedia Act (TMG), Article 2 lit. b of the EC Directive and Article 1 (1) of Directive 2015/1535 , the technical process of providing access is irrelevant for a service to be considered an information society service and also a telemedia service. There is also no need for a broader interpretation (statement of defense dated July 29, 2022, p. 26f.).

2. materiality of the incorrect assessment of the concept of "service provider

The judgment is also based on the substantial and erroneous assessment of the concept of service provider, since if the defendant had been appropriately considered as an access intermediary, it would not have been entitled to injunctive relief pursuant to Section 8 (1) sentence 2 of the German Telemedia Act (TMG).

3. privileged liability of the defendant pursuant to Section 8 (1) TMG

The Regional Court is of the opinion that the liability privilege pursuant to Section 8 (1) of the German Telemedia Act (TMG) does not apply because the defendant passes on content, does not mediate access to a network and "in any case the same" applies as for a domain registrar or an admin-c.

a. Pure pass-through / access switching by the service of the defendant

The District Court does not even begin to address the requirements of Section 8 TMG and the characteristics of the defendant's service. The Regional Court rejects the applicability of Section 8 No. 1 of the German Telemedia Act (TMG) with a single sentence and the blanket reference to the fact that "*in any case, the same*" applies to the DNS resolver as to the Admin-C or the domain registrar (Judgment, p. 10).

In doing so, the Regional Court fundamentally fails to recognize the functionality of the defendant's service, which is essentially different from that of a domain registrar and the Admin-C (statement of defense of July 29, 2012, p. 23ff.). The Federal Court of Justice does not classify registrars and Admin-C as service providers because they are not themselves involved in the technical process of retrieving a website. Their contribution consists of the one-time administrative involvement in the registration of a domain (BGH, judgment of October 15, 2020 - I ZR 13/19, para. 16 et seq. 28). This is precisely not the case with the defendant, which provides an individual service at the instigation of the user each time a website is called up and is thus continuously involved in providing access (MMR 2023, 378, 381).

The defendant's service is to be subsumed as an access broker within the meaning of Section 8 (1) TMG. As already explained, the term "access brokerage" is to be understood in a broad conceptual sense. It does not presuppose the transmission of information. If a chain of service providers is used for access provision, each service provider in the chain is privileged (statement of defence of 29.07.2022, p. 24 ff.). According to the clear provision of Art. 12 ECRL, the provision of access to a communications network is already covered by the liability privilege, not just the provision of access to the information itself (Statement of Defence of 29.07.2022, p. 25). This is the case with the defendant, which is indisputably involved in the provision of access to the DNS.

Even if the focus is on the direct transmission of information or the provision of access to a network, the defendant is to be classified as an access provider pursuant to Section 8 of the German Telemedia Act (TMG). The plaintiff asserts a claim against the defendant for the omission of the transmission of domain names and IP addresses. In the relevant facts of life of the transmission of domain names and IP addresses between the computers of the inquirers and the name servers, the defendant directly forwards information, so that it is a case of pure forwarding pursuant to §§ 2 (1), 8 TMG (Duplicik v. 31.01.2022, p. 30, MMR 2023, 378, 381).

b. Applicability of the liability privilege follows directly from the DSA

The judgment of the Regional Court lacks any discussion of the requirements of Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19, 2022 on an internal market for digital services and amending Directive 2000/31/EC, the so-called Digital Services Act (DSA). The defendant has explained in detail in the statement of defense (statement of defense dated July 29, 2022, p. 27 et seq.) and the duplicate statement (duplicate statement dated January 31, 2022, p. 25 et seq.) that the DSA clearly clarifies that the liability privilege for pure pass-through services applies to DNS resolvers.

The European legislator has reproduced the liability privileges of the E-Commerce Directive with identical wording in Art. 4 - 6 DSA; the previously applicable Art. 12 - 14 of the E-Commerce Directive are repealed, cf. Art. 89 DSA. The Digital Services Act is directly applicable as a regulation.

With the DSA, it has clarified that DNS resolver services are to be classified as pure pass-through services pursuant to Art. 4 (1) DSA with privileged liability and consequently also as service providers pursuant to Sections 2 sentence 1 no. 1 TMG, 8 (1) TMG (MMR 2023, 378, 381).

In recital 29 of the DSA, the legislator states unequivocally that DNS resolvers are among the liability-privileged services of pure transit pursuant to Art. 4 (1) DSA:

> *"Intermediary services encompass a wide range of economic activities that take place online and continue to evolve to enable the rapid, secure, and protected transmission of information and provide convenient solutions to all stakeholders in the online ecosystem. Switching services of a '**pure pass-through**' nature include, for example, general categories of services such as Internet exchange nodes, wireless access points, virtual private networks, **DNS services and DNS resolvers,** top level domain name registry services, registrars, certification authorities issuing digital certificates, Internet voice telephony (VoIP), and other interpersonal communications services; [...]" (emphasis by the undersigned)*

The fact that the European legislator did not intend to bring about a constitutive change in the law, but merely to clarify the current legal situation with regard to technical developments since the E-Commerce Directive came into force, which has been continued with the same wording, is also clear from recital 28:

> "*In this regard, it should be **recalled** that providers of services to provide and facilitate the underlying logical architecture and smooth functioning of the Internet, including auxiliary technical functions, may also benefit from the exclusions of liability set out in this Regulation, provided that their services are classified as a 'mere conduit', 'caching' or 'hosting' service. Such services include, but are not limited to, wireless local area networks (WLANs), **DNS services** [...]" (emphasis by the undersigned)*

The Digital Services Act entered into force on November 22, 2022, and applies in full from February 17, 2024, in accordance with Art. 93 DSA. The date set for the applicability of the Act, for example with regard to individual facts, certain assessment periods or certain fiscal years, may differ from the effective date. Application provisions tend to have the function of

transitional provisions (Handbook of Legal Formalities, 3rd edition, Part C, 11 Applicability Time Rules, 11.1 Effective Date Rules, marginal no. 438).

Laws take effect when they come into force. They shape the legal system for the future and therefore regularly cover all legal relationships that arise in the future. However, a new law can also affect existing legal relationships. In this case, there are differences depending on whether the circumstances are closed or still open. Transitional provisions clarify the effects of the law or individual regulations, modify them or give them special form with a view to the intended future order (Handbuch der Rechtsförmlichkeit, 3rd edition, Part C, marginal no. 412). The start-up period established after the entry into force of the DSA merely serves to ensure that the affected intermediary services have sufficient time to achieve the intended legal status, as this may result in significant technical changes to systems that cannot be fully achieved immediately. Accordingly, the start-up time of the DSA refers to the action obligations of the switching services. The scope of the regulation for switching services according to Art. 2 DSA already applies when the regulation enters into force, from which it follows that DNS resolvers as switching services are covered by the scope. This follows unambiguously from the recitals mentioned above.

In its reply (reply dated March 31, 2023, p. 26 f.), the defendant explained on the basis of the expert opinion of Prof. Dr. Ruth Janal, submitted as Annex B 13, that the DSA has a preliminary effect and that the legislative assessments must already be taken into account by the courts of the Member States. It follows from the prohibition of frustration under Union law from Article 4 (3) TEU that the Member State authorities are obliged to avoid measures that are likely to seriously jeopardize the objectives of the Union legal act. A claim by a DNS resolver for an injunction against the resolution of certain domain names under Section 97 (1) UrhG is directed to the future. A corresponding injunction would thus be likely to seriously jeopardize the effect of Art. 4 (1) DSA unless it is limited in time to the beginning of the temporal scope of application of the DSA (Annex B13, p. 14 f.).

Consequently, the District Court should not have ignored recital 29 of the DSA as pointed out by the defendant, but should have taken it into account when subsuming the interpretation of the question of application of Section 8 of the German Telemedia Act (TMG) to the liability privilege.

c. Unequal treatment with access providers leads to valuation contradictions

The legal opinion of the Regional Court that DNS resolvers cannot invoke the liability privilege pursuant to Section 8 (1) of the German Telemedia Act (TMG) leads to inconsistencies in valuation and unequal treatment with Internet access providers that is not objectively justified (statement of defense of July 29, 2022, p. 28f.; response of March 31, 2023, p. 27f., Annex B13, p. 12f.).

Internet access providers always provide DNS resolver services as part of their service. The resolution of IP addresses into domain names is part of the uniform fact of life of the provision of Internet access services. Internet access providers are indisputably privileged with regard to liability for these services pursuant to Section 8 No. 1 TMG. This privilege must also include DNS resolver services, as otherwise the liability privilege would be void (statement of defense

of July 29, 2022, p. 28f; reply of March 31, 2023, p. 27). Internet access providers also implement DNS blocks, which were, for example, the subject of the Federal Court of Justice (BGH) decision "DNS-Sperre" (BGH, judgment of October 13, 2022 - I ZR 111/21, GRUR 2022, 1812- DNS-Sperre), by configuring the DNS resolvers they operate. If the DNS query step is not included in the technical facts of life of access provision, the privileges for access providers pursuant to Section 8 (1) of the German Telemedia Act (TMG) would be rendered meaningless, since the providers would then be exposed to liability and audit risks not in their capacity as access providers, but in their capacity as providers of a recursive DNS resolver (statement of defense of July 29, 2022, p. 27f.).

Excluding the operation of DNS resolvers from the liability privilege pursuant to Section 8 of the German Telemedia Act (TMG) not only leads to inconsistencies in valuation, but also to unequal treatment that is not objectively justified. Prof. Janal explains:

> *"Access providers who offer DNS resolving as part of their service are privileged from liability within the limits of Section 8 (1) of the German Telemedia Act (TMG) and can only be held liable for blocking access to a domain pursuant to Section 7 (4) of the TMG. In this context, the blocking request is usually directed at the establishment of a DNS block, i.e., to refrain from resolving certain domain names. In contrast, according to the Cologne Regional Court, providers of independent DNS resolvers are to be liable as perpetrators of copyright infringement if they do not stop the resolution of the aforementioned domain names in response to a blocking request from a rights holder. Accordingly, the same behavior - performing the DNS lookup - is treated differently. For this unequal treatment between access provider and independent DNS resolver, no factual reasons are given in the case law of the courts of instance that are appropriate to the differentiation goal and the extent of the unequal treatment. For example, the assertion that the liability privileges of the Telemedia Act are to be interpreted narrowly is not a factual reason for differentiation. Likewise, no appropriate factual reason can be identified for subjecting an "ancillary service" to stricter liability than a main service. Nor does the fact that access brokers offer an additional service, namely the provision of access to the Internet and the transmission of the content stored under the IP address, constitute a factual reason for privileging an access broker. This is because both services are indispensable for the use of the World Wide Web. On the contrary, the access broker is "closer" to the infringement than the resolution of the IP address by a resolver, because potentially infringing content is transmitted by the access broker, but not by the DNS resolver. This argues for stricter liability of the access provider over an independent DNS resolver, not stricter liability of the DNS resolver." (Exhibit B13, p. 13 with further references).*

4. no perpetrator liability of the defendant

The Regional Court ordered the defendant as the perpetrator of a copyright infringement pursuant to Section 97 (1) UrhG to cease and desist from dissolving the disputed domain name. In doing so, the Regional Court assumes in an unjustifiable manner that the defendant is making a public reproduction of the sound recordings in dispute by operating the DNS resolver service (judgment, p. 11 f.).

The Regional Court assumes that the performance of an intermediary activity and the mere knowledge of an infringement on a platform operated by a third party are sufficient for the act of communication to the public. This view fundamentally ignores the systematics of the liability privileges of the TMG and the ECRL. It is not compatible with the case law of the Federal Court of Justice and the European Court of Justice on hosting and intermediary services.

The Regional Court transfers the case law of the ECJ on certain hosting services (see ECJ, Judgment of 22 June 2021, Cases C-682/18 and C-683/18, para. 75 - YouTube/Cyando) to the DNS resolver service of the defendant in one sentence. The District Court states apodictically that the defendant plays a central role in the claimed copyright infringement by resolving the domain name into an IP address (Judgment, p. 11). In doing so, the Regional Court fails to recognize that the ECJ's statements refer to certain categories of hosting services, namely a video and a share hosting platform. In doing so, the Regional Court fails to recognize that this case law cannot be easily applied to the technically completely different situation of resolving DNS queries. The District Court's statement that the remarks were not "exclusively limited to the case of the host provider" (Judgment, p. 11) does not relieve the District Court from examining whether the defendant's performance constitutes communication to the public pursuant to Article 3 (1) of the InfoSoc Directive.

The opinion of the Regional Court that the defendant is engaged in communication to the public because it plays a central role in the infringement and acts intentionally meets with serious reservations. The decision of the ECJ in the case of YouTube/Cyando does not provide any generalizable standards for the criteria to be used to assess the act of communication to the public by other service providers or other information society intermediaries. Both the ECJ and the Federal Court of Justice make a strict distinction in their case law between the different types of service providers. The ECJ has always considered Internet access providers and providers of intermediary services and intermediary services as intermediaries pursuant to Art. 8 (3) InfoSoc Directive, Art. 12 E-Commerce Directive and not as perpetrators of the act of communication to the public (ECJ, judgment v. 27 March 2014 - C-314/12, GRUR 2014, 468 - UPC Telekabel; ECJ, Judgment v-. 15 September 2016 - C-484/14, GRUR 2016, 1146 - McFadden, Duplicik v. 31.03.2023, p. 22, Annex B13, p. 7f.). There are no indications that the ECJ intended to deviate from this case law in the YouTube/Cyando decision. Accordingly, the Federal Court of Justice also clarifies in the YouTube II and Uploaded III decisions (Federal Court of Justice, judgment of June 2 .2022 - I ZR 140/15, para. 112 - YouTube II; Federal Court of Justice, judgment of June 2, 2022 - I ZR 135/18, - Uploaded III) that it only changed its case law on communication to the public by means of intermediary services with regard to host providers. This is clear from the passages of the reasons for the decision referred to by Prof. Janal (Annex B13, p. 8 f.). The decisions of the Federal Court of Justice are obviously limited to the constellations at issue, as can be seen from the phrases "in such a case", "in this constellation" and "here, liability as a perpetrator replaces the previous "Stoererhaftung" (Breach of Duty of Care). For service providers other than host providers, the decisions contain no statement (Annex B13, p. 9 with further references and reference to Ohly, NJW 2022, 2961, 2962 f.).

The opinion of the Regional Court also contradicts the case law of the Federal Court of Justice (BGH) in the DNS blocking decision (BGH, judgment dated October 13, 2022 - I ZR 111/21 - DNS blocking). The BGH examines the liability of the Internet access provider solely from the perspective of Section 7 (4) TMG. The Federal Court of Justice does not consider the Internet

access provider to be criminally liable if it fails to set up a DNS block after being notified of infringing content.

The statements of the ECJ and the BGH on the central role of certain hosting providers cannot be transferred to DNS resolvers. The ECJ and the BGH derive the central role of these services in particular from their special access possibilities, since the infringing content is in their sphere and hosting services can terminate this content specifically and completely. The "central role" in making works accessible required by the ECJ can therefore be present in the case of these service providers if operators of an online file-sharing platform offer their users access to the works in question by making them available and operating them (ECJ, Judgment of 22 June 2021, Cases C-682/18 and C-683/18, - YouTube/Cyando, para. 77). The ECJ focuses on the fact that the direct perpetrator is a user of the hosting service and that the protected content is made accessible via the service of the hosting provider (ECJ loc. cit. para. 77, 83, 84). The role of the DNS resolver is fundamentally different. A DNS resolver acts as an intermediary that retrieves and passes on the request for a domain or IP address (statement of defense of July 29, 2022, p. 2). The protected objects are neither in the sphere of access of the DNS resolver, nor do the perpetrators of the infringements use the defendant's service to make protected content publicly accessible in an unlawful manner. The Defendant's service does not store any information, the service is limited to the transmission of information (IP addresses and domain names). Moreover, unlike host providers, the defendant cannot delete and block content in a targeted manner; a block in the defendant's service always affects all content in a domain (Statement of Defence of 29.07.2022, p. 38, Duplicate of 31.03.2023, p. 40).

The opinion of the Regional Court that the reference to an (alleged) infringement on a third-party platform constitutes intent with regard to an act of communication to the public (judgment, p. 11) also meets with serious reservations. The Regional Court fails to recognize the systematics of the liability privileges of the German Telemedia Act. The liability privilege for host providers does not apply pursuant to Section 10, sentence 1, no. 2 of the German Telemedia Act (TMG) if they have been made aware of infringing information and do not delete it immediately. The liability privilege for access providers pursuant to Section 8 (1) TMG does not include such a duty to respond. The liability privilege therefore also applies in principle if the service provider has positive knowledge of the illegal information (Annex B13, p. 7f.). If the lack of remedial action by such a service were to be interpreted as an act of communication to the public in accordance with the opinion of the Regional Court, this would have the consequence, according to the decision, that the service provider could not invoke the liability privilege. However, this would counteract and circumvent the liability privileges specifically tailored to these service providers.

Irrespective of this, public reproduction by the defendant cannot be considered, if only for the reason that the defendant implemented a blocking of the disputed domain limited to the territory of the Federal Republic of Germany by means of a geographical allocation of the IP addresses after the conviction by the Regional Court of Hamburg in the preliminary injunction proceedings. In this respect, it has taken the "necessary measures" to bring about the injunction sought by the plaintiff to dissolve the domains in dispute for the territory of the Federal Republic of Germany (Duplicik v. 30.01.2023, p. 23f.). The fact that the geographically limited blocking can be specifically circumvented by the use of VPN software does not prevent it from being effective (see Statement of defense of July 29, 2022, p. 23). In the opinion on the Grand Production proceedings (ECJ, C-423/21 - Grand Production, opinion of 20.12.2022), Advocate General Szpunar states that there is no communication to the public in the case of

geographical access blocks for the areas for which the block is implemented. An exception to this only applies if the respective service intentionally applies an ineffective geographical access barrier (ECJ, loc. cit., para. 36 et seq.; 44).

This is obviously not the case here; the defendant has set up an access barrier in accordance with the highest technical standards. Accordingly, the intentional concealment of the whereabouts through the use of a VPN service by the witness Kunath does not lead to a reproduction act by the defendant. A communication to the public by the defendant is therefore ruled out already for the reason that the defendant has no intent to enable a reproduction act on the territory of the Federal Republic (Duplik v. 30.01.2023, p. 24). The Leipzig Regional Court also did not address this argument.

5. worldwide DNS blocking disproportionate

The assumption of the Regional Court that it would be harmless if the defendant blocked the domains in dispute globally for all Internet users, irrespective of the applicable law in each case (judgment, p. 12) also meets with far-reaching reservations.

The "objections of the defendant" briefly mentioned by the Leipzig Regional Court and the assessment that these do not preclude a claim (Judgment, p. 12) makes it clear that the Regional Court did not even begin to address the defendant's submission (Statement of Defence dated 29.07.2022, p. 9).

The defendant has repeatedly referred to the established case law of the ECJ and the Federal Court of Justice that blocking measures against copyright infringements must always be strictly target-oriented (statement of defense of July 29, 2022, p. 39f; Federal Court of Justice, judgment of November 26, 2015 - I ZR 174/14, GRUR 2016, 268, marginal no. 53 - Störerhaftung des Access Providers; ECJ, judgment of March 27, 2014 - C-314/12, GRUR 2014, 468, marginal no. 63- UPC Telekabel). A blocking measure must not result in disproportionate impairment of Internet users' access to lawful information.

The blanket assertion that overblocking is harmless because there is no legitimate interest worldwide in accessing this website (judgment, p. 12) extends the legal consequences of Article 8 (1) of the Rome II Regulation to an unjustifiable extent. According to the plaintiff's submission, its rights are limited to the territory of the Federal Republic of Germany (action of 22.04.2022, p. 15). Accordingly, the plaintiff is not entitled to injunctive relief outside the Federal Republic of Germany.

The defendant stated in the statement of defense (statement of defense dated July 29, 2022, p. 41 et seq.) that due to the worldwide blocking effect there is an increased risk that access to information that is not prohibited in other jurisdictions is prevented. In this context, it is independent of whether the infringing content accessible via the disputed domain is also illegal in the legal systems of the TRIPS member states; the question must be assessed according to whether the respective legal systems would have permitted a claim against the defendant. As explained, court orders against DNS resolvers have so far remained isolated cases internationally (see Schwemer, Copyright Content Moderation at Non-Content Layers, in: Rosati, Handbook of European Copyright Law (2021), p. 11). At this point, the District Court also does not address the defendant's arguments (statement of defense of July 29, 2022, p.

41 et seq.) that, for example, for reasons of proportionality and subsidiarity, recourse to DNS resolvers is not possible under other legal systems. Under Swiss law, where the defendant is domiciled, access intermediaries cannot be held liable for the establishment of DNS blocks based on copyright infringements for lack of their own contribution to the crime (Federal Court, judgment of February 4, 2019, 4A_433/2018). The worldwide blocking effect leads to the occurrence of a legal consequence that is not provided for under other legal systems or, as in the case of Switzerland, is expressly excluded. The Respondent pointed out that Member States must ensure that the measures they adopt are compatible with international law (id. at para. 52). Accordingly, whether an order with extraterritorial effect is permissible under international law must first be determined in the individual case and cannot be asserted in a blanket manner by the Regional Court. However, the admissibility of extraterritorial orders is generally to be denied under international law outside of special permissions (in particular international treaties) (cf. Krämer, EuR 2021, 137, 138). The Regional Court does not comment on the permissibility of blocking with worldwide effect under international law.

6. no judicial means of legal protection

The Regional Court did not consider that, according to the case law of the ECJ and the Federal Court of Justice, the lawfulness of a DNS block requires that the Internet users affected have an effective judicial remedy to assert their rights in court after becoming aware of the blocking measures taken by the provider (ECJ, judgment of. March 27, 2014 - C-314/12, GRUR 2014, 468, para. 56 - UPC Telekabel; BGH, judgment of November 26, 2015 - I ZR 174/14, GRUR 2016, 268, para. 57 - Access provider's liability for interference). The Regional Court did not address the fact that the defendant explained in detail that there is no legal remedy available to Internet users in this case that would enable them to have the DNS block reviewed by the courts (statement of defense of July 29, 2022, p. 38 f.; reply of January 30, 2023, p. 33).

7. no entitlement to take "reasonable precautionary measures".

With reference to the Uploaded III decision (BGH, judgment of June 2, 2022 - I ZR 135/18- Uploaded III), the Regional Court requires the defendant to "take reasonable precautionary measures to prevent the uploading of files with comparable infringing content in the future" (judgment, p. 12). These statements prove that the Regional Court fundamentally misunderstood the functionality of the Defendant's service and, again, unseeingly wants to transfer the case law of the Federal Court of Justice on hosting providers to the Defendant's DNS resolver service. This fundamental misunderstanding of the District Court becomes particularly clear in the transfer of the principles on taking precautionary measures: because unlike the sharehosting service involved in the Uploaded III proceedings, the defendant cannot prevent the uploading of files, since the uploading of files on the defendant's service is simply not possible. The defendant does not store any information, including the sound recordings in dispute, as explained several times (Statement of Defence of 29.07.2022, p. 2; Duplicik of 30.01.2023, p. 6 et seq.). The service of the defendant consists solely in the transmission of domain names and IP addresses.

8. no blocking claim pursuant to Section 7 (4) of the German Telemedia Act (TMG)

The Regional Court, although it would not be obliged to do so due to the assumption of perpetual communication to the public by the defendant, at least partially examines the requirements of Section 7 (4) TMG. In doing so, the Regional Court erred in law in assuming that the plaintiff had made sufficient efforts to give priority to parties closer to the act (judgment, p. 13 f).

a. Utilization excluded due to subsidiarity

In its DNS blocking decision, the Federal Court of Justice (BGH) once again clarified that the blocking of a website is subject to strict requirements and that the blocking claim pursuant to Section 7 (4) of the German Telemedia Act (TMG) can only be considered as ultima ratio if the rights holder has previously exhausted all reasonable possibilities of taking recourse to parties closer to the offence. In this decision, the Federal Court of Justice clarifies that the rights holder can reasonably be expected to make considerable efforts to eliminate the infringement by parties closer to him, taking into account his economic resources. The BGH first confirms its principles developed in the context of "Stoererhaftung" (Breach of Duty of Care) on the subsidiary claim of access providers (BGH ZUM 2016, 349, para. 83 - Stoererhaftung des Access-Providers; BGH ZUM 2021, 148, para. 27 - Breach of Duty of Care of the Registrar), according to which the rights holder can reasonably be expected to involve state investigative authorities and private detectives as well as to assert claims for information against the host provider in order to determine the identity of the operators of the website (cf. in detail statement of defense of July 29, 2022, p. 21, 33; duplicate of January 30, 2023, p. 32f.). In addition, the Federal Court of Justice clarifies that the rights holder must in principle first assert a third-party right to information against host providers located in other EU countries before a court in the Federal Republic of Germany:

> *"Which efforts to claim the operator of the Internet site and the host provider are reasonable is a question of the individual case.*
>
> *(1) The rightholder shall be obliged to a reasonable extent to conduct investigations to identify the parties whose claims have priority (cf. BT-Drucks. 18/12202, p. 12). This includes, in particular, the* ***involvement of state investigating authorities by way of a criminal complaint*** *(cf. BGHZ 208, 82 [juris marg. no. 87] - "Stoererhaftung" (Breach of Duty of Care) of the access provider) and the extrajudicial assertion of a claim for third-party information against the host provider in order to identify the operator of the website. The* ***conduct of private investigations, for example by a detective*** *or other companies that carry out investigations in connection with illegal offers on the Internet, is also reasonable in principle - taking into account the economic resources of the rights holder (see BGHZ 208, 82 [juris, marginal no. 87] - Breach of Duty of Care of the Access Provider).*
>
> *(2) As a rule, the right holder can also be reasonably expected to make an out-of-court claim against a known operator of the Internet site or host provider for the removal of the copyright-infringing content.*
>
> *[...]*

> ***However, the right holder must in principle initiate proceedings for interim relief against operators or host providers located within the European Union*** *(cf. Spindler, GRUR 2014, 826, 832; ibid., GRUR 2016, 451, 458; also J. B. Nordemann in Fromm/Nordemann aaO Section 97 no. 171a; probably also Weisser/Färber, BB 2016, 776, 777). Against the background of the trust that the Member States of the European Union place in each other's legal systems and judicial organs (cf. also BGH, Order of November 17, 2021 - I ZB 16/21, IWRZ 2022, 129 [juris para. 39 cit.]), it can generally be assumed that an interim injunction can be obtained and enforced quickly within the European Union.* ***However,*** *insofar as countries outside the European Union are concerned,* ***the existence of equivalent legal protection options must be examined in the individual case*** *without imposing excessive burdens of proof on the applicant (see Spindler, GRUR 2014, 826, 832; Leistner/Grisse, GRUR 2015, 105, 107 f.).*
>
> *[...]*
>
> *The assessment of reasonableness also takes into account the fact that the plaintiffs are large and internationally active scientific publishers who hold rights to a large number of works.* ***With a view to preventing future infringements, it is in their own interest to determine the identity of the operators of the Internet services*** *(cf. BGH, judgment of May 12, 2010 - I ZR 121/08, BGHZ 185, 330 [legal nos. 22 and 34] = GRUR 2010, 633 - Sommer unseres Lebens).*" (BGH, judgment of October 13, 2022 - I ZR 111/21, GRUR 2022, 1812 - DNS-Sperre, nos. 38 et seq., 55) (emphasis added by the undersigned).

The defendant has submitted in detail that the plaintiff did not take any of the measures it could reasonably be expected to take under this case law. Neither did the plaintiff file a criminal complaint, nor did it call in a private investigator, nor did it attempt to assert a judicial claim for third-party information against the host provider based in the EU by way of urgent legal protection, nor did it submit information on legal protection options at the host provider's registered office in Ukraine, nor did it make sufficient efforts to call in other parties closer to the offence (statement of defense v. 29.07.2022, p. 33 ff.; duplicate v. 30.01.2023 , p. 31 ff.).

The Regional Court errs in law in assuming that the plaintiff could not reasonably be expected to assert a claim for third-party information in court (judgment, p. 14). There is no discussion of the other subsidiarity requirements of the Federal Court of Justice (BGH, loc. cit. para. 38).

The Regional Court fails to recognize that, according to the case law of the Federal Court of Justice, proceedings for interim legal protection may only be omitted if the action lacks any prospect of success for reasons to be explained by the claimant (Federal Court of Justice, loc. cit. para. 42). The plaintiff has not been able to demonstrate this to any extent. The plaintiff did not establish until the court proceedings that it had not made sufficient claims against the host providers. Therefore, with its submission (Replik v. 17.10.2022, p.18) that a third party was unable to deliver a letter through a courier in a different matter a month before the defendant made a claim, it is trying to create the impression that delivery is not promising. It cannot be concluded from this submission that a judicial claim lacks any prospect of success. Accordingly, the Federal Court of Justice also makes a clear distinction between the requirement of out-of-court recourse (Federal Court of Justice, loc. cit. para. 40) and the

additional requirement of recourse to the courts (Federal Court of Justice, loc. cit. para. 42) with possible official service within the EU.

From which the Regional Court draws the conclusion (judgment, p. 14) that the address of the host provider in Lithuania and thus the EU cannot be determined remains open. The defendant has submitted that the host provider is entered in the commercial register at the address stated in the imprint, and has regularly reported sales and employees subject to social security contributions there in recent years (duplicate dated January 30, 2023, p. 32, Exhibit B23). The defendant already argued in the duplicate (duplicate dated January 30, 2023, p. 32) that it would have been open to the plaintiff to have the injunction executed by a Lithuanian bailiff in accordance with the EU Regulation on service in civil and commercial matters (Regulation (EU) 2020/1784). Beyond the single, unsuccessful attempt at service, which moreover took place a considerable time ago since the action was filed, the plaintiff cannot assume that a renewed service or an official service by means of the bailiff does not promise success (MMR 2023, 378, 381).

Finally, the plaintiff's action in the preliminary injunction proceedings against the defendants shows that court service has a special quality compared to private attempts at service. In its statement of claim, the plaintiff stated that the defendant had thwarted postal service of the preliminary injunction issued by the Hamburg Regional Court by providing an incorrect address in the masthead, (action dated April 22, 2022, p. 10). However, this did not prevent the plaintiff from applying for an injunction against the defendant and having it served outside the EU with the help of the Hamburg Regional Court. It must then also follow from the principle of subsidiarity that an injunction must first be applied for against the host provider and an attempt made to have it served, if necessary with the help of court service, before legal action is taken against a service that can only be claimed as a subordinate service, if at all, and is also located outside the EU.

With regard to the attempted service in Ukraine, the refusal of acceptance submitted by the plaintiff was sufficient for the Leipzig Regional Court to declare the priority claim to have failed (judgment, p.14). The Regional Court does not observe the requirements of the Federal Court of Justice to also examine the possibilities of judicial recourse in countries outside the EU. However, enforcement of German court judgments in Ukraine is possible even without the conclusion of an international treaty on legal assistance (https://berlineranwaltsblatt.de/ce/deutsche-gerichtsurteile-in-der-ukraine/detail.html).

The opinion of the Regional Court that the possibilities of a claim are exhausted if a provider who is indisputably resident at an address merely refuses service would lead to the priority claim of providers who are closer to the act, as required by the Federal Court of Justice, being undermined. It would then be up to the provider with priority to evade responsibility and place the burden of action on the provider furthest away from the offence. This would lead to inappropriate results, as has happened here.

In addition, the Regional Court ignores the entire submission of the defendant on the lack of recourse to other parties closer to the offence (statement of defense dated July 29, 2022, p. 21 et seq. and reply dated January 30, 2023, p. 33) and does not acknowledge this in any way. An explanation in the reasons for the judgment of the Regional Court as to why a claim against these parties cannot be considered is also completely missing. In particular, the Regional Court

did not acknowledge that no measures were taken by the plaintiff vis-à-vis RIPE either to obtain correct contact data so that successful service could be effected or to have the IP addresses used for the alleged infringement revoked from the host provider (Duplicik v. 30.01.2023, p. 31).

The defendant also already expressly pointed out (duplicate dated January 30, 2023, p. 32) that neither the plaintiff's representative nor proMedia GmbH, which it commissioned to document the asserted infringement, are "private investigators", the use of which was required by the Federal Court of Justice in the decision *Störerhaftung des Access Providers* (BGH, judgment dated November 26, 2015 - I ZR 174/14, GRUR 2016, 268, marginal no. 87 - Störerhaftung des Access Providers). In this decision, the Federal Court of Justice expressly required the use of private investigators or the involvement of state investigating authorities to take measures that go beyond the measures outlined by the plaintiff to determine the identity of the website operators. Accordingly, the BGH names private investigators or companies that conduct investigations in connection with infringements of rights on the Internet as an example of "private investigators" (BGH loc. cit.). The Regional Court did not address the deficiencies of the investigation attempts and the insufficient circumstances of the one-time delivery attempt in the reasons for the judgment, despite sufficient monition by the defendant.

b. Utilization excluded due to disproportionality

In its examination of Section 7 (4) of the German Telemedia Act (TMG), the Regional Court did not take into account the fact that the standard requires an examination of the proportionality and reasonableness of the blocking measure. The Regional Court does not appreciate the defendant's detailed submission on the disproportionality of setting up a DNS block due to the effects on the performance of the defendant's system and business operations (statement of defense of July 29, 2022, p. 12 et seq. 41 et seq. ; Duplicik v. 30.01.2023, p. 7ff, 35) nor the detailed submission of the defendant on the disproportionality of the DNS block due to the interference with the freedom of information of the inquirers of the defendant (statement of defense v. 29.07.2022, p. 39 ff; Duplicik v. 30.01.2023, p. 33 f.).

In addition, reference is made to all submissions made at first instance.

The judgment of the Leipzig Regional Court must be set aside and the action dismissed in its entirety.

C. Admission of the appeal

Admission of the appeal is requested with regard to the need to further develop the law or to ensure uniformity of case law pursuant to Section 543 (2) sentence 1 no. 2 of the German Code of Civil Procedure (ZPO). The legal dispute touches on issues on which the Federal Court of Justice has not ruled or has not ruled conclusively (e.g., the question of the culpability of liability-privileged service providers in the case of failure to block domain names without delay).

D. Transfer of the case to the single judge

Since the legal dispute raises questions that have not yet been conclusively clarified in the case law of the highest courts, it does not appear appropriate to transfer the case to the single judge pursuant to Section 526 (1) No. 2 of the Code of Civil Procedure (see Wieczorek/Schütze/Gerken, loc.cit., Section 526 No. 5; Thomas/Putzo/Seiler, loc.cit., Section 526 No. 7).

Rickert Law Firm Ltd.
by:

Thomas Rickert
(Lawyer)