



Leipzig District  
Court

Civil Chamber

File number: **05 O 807/22**

## IN THE NAME OF THE PEOPLE

### FINAL JUDGMENT

In the litigation

████████████████████████████████████████████████████████████████████████████████  
████████████████████████████████████████████████████████████████████████████████

- Plaintiff -

Litigation Counsel:

████████████████████████████████████████████████████████████████████████████████

against

**Quad9 Foundation**, c/o Switch, Werderstrasse 2, 8004 Zurich, Switzerland  
represented by d. Trustees

- Defendant

-

Litigation Counsel:

**Rickert Rechtsanwaltsgesellschaft mbH**, Colmantstraße 15, 53115 Bonn

for injunction

the 5th Civil Chamber of the Regional Court of Leipzig by

Judge at the Regional Court ██████████ as single judge

Based on the oral hearing of 08.02.2023 on 01.03.2023

**found to be right:**

1. The defendant is ordered to avoid a fine to be determined by the court for each case of infringement and, in the event that this cannot be recovered, to be imprisoned for up to 6 months (fine in each case not exceeding € 250,000.00, imprisonment for a total of not more than two years).

to refrain from selling on the territory of the Federal Republic of Germany the music album

"Evanescence - The Bitter Truth"

with the sound recordings contained thereon

1. Artifact/The Turn 2. Broken Pieces Shine 3. The Game Is Over 4. Yeah Right 5. Feeding the Dark 6. Wasted on You 7. Better Without You 8. Use My Voice 9. Take Cover 10. Far From Heaven 11. Part of Me 12. Blind Belief

to be made publicly available,

by the Defendant providing its users with a DNS resolver service, which does- main

"██████████"

and/or the subdomain "██████████".

translated into numeric IP addresses,

so that it is possible for the users of the defendant with the help of these numerical IP addresses to reach the Internet service under the domain "██████████" and/or the subdomain "██████████" and/or the further domain(s) and to call up there links to unlawful storage of the album,

as happened

by the defendant offering its users the DNS resolver service "Quad9" at the IP address 9.9.9.9, with the help of which the users for the in the attached attachment

K 36 depicted contribution and the Internet address

[http://\[REDACTED\]](http://[REDACTED]),

as well as the article reproduced in the attached Annex K 37 and the Internet addresses

[http://\[REDACTED\]](http://[REDACTED]),

[http://\[REDACTED\]](http://[REDACTED]) and

[http://\[REDACTED\]](http://[REDACTED])

numeric IP addresses were transmitted,

which enabled them to access the hyperlinks provided at the aforementioned addresses to the storage locations of

[http://\[REDACTED\]](http://[REDACTED])

[REDACTED].

[http://\[REDACTED\]](http://[REDACTED])

and call up the illegally stored copies of the aforementioned album.

2. Of the costs of the proceedings, the plaintiff shall bear 20% and the defendant 80%.

3. The judgment is provisionally enforceable for the plaintiff against security in the amount of 100,000.00 euros and for the defendant against security in the amount of 110% of the respective amount to be enforced.

**Decision:**

The amount in dispute is set at EUR 100,000.00.

## Facts

The parties are disputing a DNS blocking for the benefit of a copyright holder in main proceedings following previous preliminary legal protection proceedings.

The facts in dispute were the subject of preliminary injunction proceedings before the Hamburg Regional Court under file no. 310 O 99/21, in which the order was issued and confirmed by judgment (Annex K1, K2).

The plaintiff is a German producer of sound recordings. The Defendant is a foundation based in Switzerland and operates an open recursive DNS resolver that provides a free domain name resolver for Internet end users at the IP address 9.9.9.9 ("Quad9"). The Domain Name System (DNS) is used to translate text-based queries, especially for Internet sites, into IP addresses and can therefore be compared to a telephone directory in the broadest sense. If a user at his Internet access enters a domain name in the address line of the Internet browser to call up the page, a DNS lookup first takes place - if the IP address is not already cached in the device. The terminal asks the preset DNS server for the IP address for the domain. The device responds to the request from its memory or connects to one or more DNS servers in the background to query the IP address there. Only in the second step does the user's web browser connect to the server at the IP address communicated to it in order to call up the website. Here, the defendant's offer can be set as a standard DNS resolver.

Music content is listed and categorized under the domain [www.██████████](http://www.██████████). The parenthesis of the website is "██████████".

The plaintiff alleges that ██████████ is a structurally copyright-infringing website on which music and radio play albums are offered for download without the consent of the rightholders. According to a study by the company ██████████ ██████████, the total number of offers on January 8, 2021, amounted to a total of 49,239 products of music, music video and radio play releases. An expert evaluation of the offerings had come to the conclusion that they were almost exclusively

unauthorized publications of protected sound and video recordings. The plaintiff is the producer of the sound with regard to the album "Evanescence -The Bitter Truth". This album was released on March 26, 2021, but could already be found on [REDACTED] on March 13, 2021. In a letter dated March 23, 2021, the plaintiff drew the defendant's attention to the infringement and also pointed out the URL. The defendant was requested to put an end to the infringement. The defendant was warned after it failed to remedy the situation.

The plaintiff had made every conceivable effort to remove the infringing offer with the involvement of primarily liable parties. The [REDACTED] website has no imprint. Entries on the domain owner were also not available. Requests for deletion to the host provider remained unanswered. There 2 IP addresses were named. The company [REDACTED] with an administrative and technical contact in the Ukraine was identified as the responsible organization. The company was allegedly based in Vilnius (Lithuania). There, however, a delivery by courier could not take place due to the lack of a traceable signature. In Ukraine, delivery was not possible because the address was located in a high-security area to which it was not possible to accept deliveries without express consent; this consent had been refused here.

The plaintiff is of the opinion that the defendant is liable as a tortfeasor. According to recent case law, it is also liable as the perpetrator of a copyright infringement. The defendant could not rely on difficulties or financial hurdles in setting up blocks, since the type of blocking was subject to its own decision and there was no apparent reason for technically carrying out a block only in regional terms.

After a partial withdrawal at the oral hearing, the plaintiff lastly claimed:

1. the defendant is ordered to avoid a fine to be determined by the court for each case of infringement and, in the event that this cannot be recovered, to be imprisoned for up to 6 months (fine in each case not exceeding € 250,000.00, imprisonment for a total of not more than two years)

to refrain from selling on the territory of the Federal Republic of Germany the music album

"Evanescence - The Bitter Truth"

with the sound recordings contained thereon

1. Artifact/The Turn 2. Broken Pieces Shine 3. The Game Is Over 4. Yeah Right 5. Feeding the Dark 6. Wasted on You 7. Better Without You 8. Use My Voice 9. Take Cover 10. Far From Heaven 11. Part of Me 12. Blind Belief

to be made publicly available,

By the Defendant providing its users with a DNS resolver service that includes the domain "██████████" and/or the sub-domain "██████████".

translated into numeric IP addresses,

so that it is possible for the Defendant's users, with the help of these numerical IP addresses, to reach the Internet service under the domain "██████████" and/or the subdomain "██████████" and/or the further domain(s) and to call up links to unlawful storage of the album there,

as happened

by the defendant offering its users the DNS resolver service "Quad9" at the IP address 9.9.9.9 with the help of which the users for the contribution shown in the attached appendix K 36 and the internet address

<http://██████████> ,

as well as the article reproduced in the attached Annex K 37 and the Internet addresses

<http://██████████> ,

<http://██████████> and

<http://██████████>

numeric IP addresses were transmitted,

which enabled them to access the hyperlinks provided at the aforementioned addresses to the storage locations of

<http://██████████> resp. <http://██████████>

and call up the illegally stored copies of the aforementioned album,

in the alternative, in the event that the court assumes a privilege pursuant to Section 8 TMG,

order the defendant to avoid a fine to be fixed by the court for each case of infringement and, in the event that this cannot be recovered, to serve a term of imprisonment of up to six months (fine in each case not exceeding € 250,000.00, imprisonment for a total of not more than two years, to be enforced on its managing director),

in its Quad9 DNS service, to block its users from accessing the Internet service currently called "[REDACTED]" as accessible through the URLs [REDACTED] and [REDACTED], by ordering the resolution of the domain "[REDACTED]" and/or the sub-domain "[REDACTED]".

in numeric IP addresses blocked, as far as over it the music album "Evanescence - The Bitter Truth" with the sound recordings contained on it 1. Artifact/The Turn 2. Broken Pieces Shine 3. The Game Is Over 4. Yeah Right 5. Feeding the Dark 6. Wasted on You 7. Better Wi- thout You 8. Use My Voice 9. Take Cover 10. Far From Heaven 11. Part of Me 12. Blind Belief

made publicly available on the territory of the Federal Republic of Germany, as done,

"in that the Defendant provides its users with the DNS resolver service „Quad9" at the IP address

9.9.9 with the help of which the users for the contribution shown in the attached attachment K 36 and the Internet address [http://\[REDACTED\]](http://[REDACTED])

[REDACTED],

as well as the contribution reproduced in the attached Annex K 37 and the Internet addresses

[http://\[REDACTED\]](http://[REDACTED]) [http://\[REDACTED\]](http://[REDACTED])

[REDACTED] and [http://\[REDACTED\]](http://[REDACTED])

[REDACTED]

received numeric IP addresses, which enabled them to link to the hyperlinks maintained at the aforementioned addresses to the locations [http://\[REDACTED\]](http://[REDACTED])

resp. [http://\[REDACTED\]](http://[REDACTED])

and call up the illegally stored copies of the aforementioned album.

The defendant requests,

dismiss the action.

The defendant claims that the specific retrieval path via the DNS resolver service of the defendant is only of minor importance in relation to the actual retrievals of the disputed domain. According to the evaluation of the Asia Pacific Network Information Centre (APNIC), the usage rate of the Respondent's service in the Federal Republic of Germany on 22.07.2022 was only 0.159% compared to 16.790% for Google. The defendant's service is characterized in particular by the fact that it offers inquirers a particularly high level of protection against IT security threats, so that, for example, malware cannot get onto the inquirers' computers. While other Internet service providers, such as host providers, can delete and block content or services precisely, DNS services only have a binary choice of options, namely to prevent the entire accessibility or non-accessibility of a domain name, combined with the risk that legitimate services or content under the domain name are inevitably also no longer accessible. The jurisdiction-related blocking of domain names is not provided for in the Respondent's system. The implementation of DNS blocking has a significant impact on the Respondent's system architecture and its performance. The plaintiff is making a claim against the defendant without first having made sufficient efforts to put an end to the asserted infringement of rights against parties closer to the defendant.

The defendant is of the opinion that the applications are too vague. The defendant is in any case privileged pursuant to § 8 I TMG. The provision of the defendant's service does not constitute an ad- equat- causal contribution to making the disputed sound recordings publicly available. A claim is excluded due to disproportionality. A perpetrator's liability according to newer criteria is ruled out, since the case law has obviously developed these specifically for the case of a host provider.

For further details, reference is made to the exchanged pleadings and annexes and to the minutes of the oral proceedings.

## Reasons for decision

The admissible action is well-founded to the extent still submitted for decision.

I.

The action is admissible.

In particular, the last request still submitted complies with the definiteness requirements of Section 253 (2) No. 2 ZPO for applications for injunctive relief. In the decision of the Federal Court of Justice of 13.10.2021, file number I ZR 111/21 - DNS - Sperre (cited in openJur), the Federal Court of Justice considered it sufficient with regard to the definiteness of the application in the case of DNS - Sperre (para. 38) that a concrete domain and the term DNS - Sperre are used. This is the case here. To the extent that the plaintiff has provided a more detailed description of the defendant's cease-and-desist obligations instead of DNS blocking, this does not harm the clarity in the aforementioned sense.

II.

The action is well-founded to the extent of the final main claim.

1.

The claims asserted by the plaintiff are to be assessed under German law. According to Article 8 (1) of Regulation (EC) No. 864/2007 on the law applicable to non-contractual obligations (Rome I Regulation), the law applicable to non-contractual obligations arising from an infringement of intellectual property rights is the law of the country for which protection is claimed.

According to this law, in particular the existence of the right, the ownership of the right by the infringed party, the content and scope of the protection as well as the facts and the legal consequences of an infringement are to be assessed (established case law; cf. BGH, judgment of September 24, 2014 | ZR 35/11, GRUR 2015, 264 - Hi Hotel II; BGH, GRUR 2016, 1048 [juris marginal no. 24] - An Evening with Marlene Dietrich, in each case with citation). As the subject matter of the action is solely claims for infringement of a

If the claimant claims that the sound recording producer's rights under Section 85 (1) sentence 1 UrhG are infringed in Germany, German copyright law is applicable in the dispute (BGH, judgment of June 2, 2022, I ZR 135/18 - uploaded III, marginal no. 21, juris).

2.

The plaintiff, as the owner of the ancillary copyrights of the sound recording producer in the Federal Republic of Germany, has the right to sue for the making available to the public of the music album in dispute. Pursuant to Section 10 (1), (3) sentence 1 UrhG, the plaintiff's right to sue for the injunctive relief relevant here must be assumed, because the plaintiff is designated as the owner of exclusive rights of use on the distribution pieces of the sound carrier containing the music album in dispute. For this purpose, the plaintiff submitted the back cover of the album (copy: Exhibit K 21). § Section 85 IV UrhG refers to the presumption of ownership under Section 10 I UrhG, which the defendant has not rebutted here.

3.

However, Section 7 IV TMG does not apply here as the basis for a claim.

According to this provision, a service provider may be subject to cease and desist obligations under Section 8 III TMG. The term "service provider" is legally defined in Section 2 No. 1 of the German Telemedia Act (TMG) as a "(...) person who makes his own or third-party telemedia available for use or provides access for use".

However, this does not apply to a DNS resolver. The term "service provider" must be defined in functional terms (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 act as a provider of services to the outside world. For example, the Admin-C is not a service provider because it only facilitates the processing of domain registrations, but neither provides information nor arranges access to it. The registrar likewise does not provide users with information or arrange access to the use of telemedia, but merely handles the administrative aspects of domain registration by providing the registry with the data required to register the domain. In particular, it is not an access broker within the meaning of Section 8 of the German Telemedia Act (TMG), because it neither provides access to a network nor forwards 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 that is the subject of the dispute here (LG Hamburg, loc. cit.).

4.

The defendant is liable in the present case as a perpetrator under Sections 97 (1), 15, 19 a, 85 UrhG.

The defendant is liable as a perpetrator because it makes its DNS resolver available to Internet users and, via this, is referred to the pages of the canna.to service with the infringing download offers relating to the music album in dispute. In this respect, the Chamber agrees with the convincing statements of the Cologne Higher Regional Court in the case 14 O 29/21, judgment of 29.09.2022 (Annex K 23 II).

a)

In this context, it is initially harmless that the plaintiff itself initially referred to the defendant's "Stoererhaftung" (Breach of Duty of Care) in its statement of reasons for the application, as it results from the development of the case law of the Federal Court of Justice up to its judgments of June 2, 2022 (I ZR 140/15 -YouTube II). It is also not necessary to decide to what extent these requirements are met cumulatively, since both justifications are directed at the same legal protection objective with identical facts.

b)

The requirements are met. In particular, the central criteria of communication to the public in the form of perpetration are fulfilled according to recent case law, namely the central role of the service provider and the intentionality of its actions (see ECJ, Judgment of June 22, 2021, Ref.: C682/18 and C-683/18 -, para. 68, juris, with further references). These are not exclusively limited to the case of a host provider.

aa)

With the DNS resolver, those users who use the defendant's resolver are first enabled to resolve a domain name into a numerical IP address and to locate the page in dispute here, which is to be seen as playing a central role in the infringement.

bb)

With regard to the intentionality of the actions, the plaintiff notified the defendant of a violation of rights with regard to the music album here. The defendant subsequently failed to comply with its duty, triggered by the infringement of the plaintiff's rights in the said music album, to take the necessary measures without undue delay in order to prevent the access to the music album.

to prevent access to this content. According to the submission of the plaintiff's representative at the hearing, which was not disputed in detail, it was possible until the end to establish a connection via the DNS resolver of the defendant to the pages mentioned in the operative part (cf. on the lack of immediacy in the case of continued availability for two days after the reference: BGH, judgment of June 2, 2022, I ZR 135/18 - Uploaded III, para. 45, juris).

cc)

The defendant's further objections also do not conflict with the claim. This is because, according to its own submission, it is also possible to filter the referral to individual domains and to block domains by also using malware according to its own submission.

dd)

It would also be harmless if, in accordance with the defendant's argument, websites were blocked globally and irrespective of a specific jurisdiction for all Internet users who use the defendant's DNS re-solver. Even worldwide, no legitimate interest of Internet users in accessing this website with obviously exclusively illegal offers is apparent, so that the question of overblocking does not arise (see OLG Cologne, judgment of October 9, 2020, Case No.: 6 U 32/20). Insofar as the defendant denies with ignorance that it is a page with (almost) exclusively illegal offers, this denial is inadmissible because the reference was concrete enough that the defendant could have recognized the character of the page by looking at the page. Moreover, the nature of the page is sufficiently proven by the submitted screenshots.

c)

aa)

On the one hand, the service provider must take reasonable precautionary measures to prevent the uploading of files with comparable infringing content in the future and, on the other hand, is also obligated to eliminate ongoing and thus future infringements (BGH, judgment of June 2, 2022 - I ZR 135/18 -, marginal no. 47, Juris). These principles apply in the same way to criminal liability for public communication within the meaning of Section 85 (1) sentence 1 case 3 UrhG in conjunction with Article 3 (2) b of Directive 2001/29/EC.

Restricting the scope of the claim to the cessation of the specific infringing act complained of would be incompatible with the requirement of effective, proportionate and dissuasive enforcement of intellectual property rights pursuant to Article 3 (2) of the Directive.

never 2004/48/EC on the enforcement of intellectual property rights, because this could circumvent the examination obligations triggered by the notice of the right holder and related enforcement measures - such as a court injunction - and deprive them of practical effectiveness (on Art. 15(1) of Directive 2000/31/EC on electronic commerce, see ECJ, Judgment of October 3, 2019 - C-18/18, GRUR 2019, 1208, cited in: BGH, Judgment of June 2, 2022

WRP 2019, 1452 - Glawischnig-Piesczek).

bb)

Thus, in the present case, too, the duty to examine triggered by the plaintiff's notice included both the duty to immediately prevent access to the specifically objected-to offer and to further similar infringing content already existing at the time of the objection and the duty to take precautions to prevent further similar infringements in the future. It is thus sufficient for the success of the application for an injunction that the plaintiff has shown that the content specifically objected to was still accessible after the notice was issued. It is not relevant whether a further similar infringement occurred thereafter (see BGH, judgment of June 2, 2022, I ZR 135/18 - Uploaded III, marginal no. 49, juris). These requirements are met here.

d)

Admittedly, the criteria restricting the claim must be complied with, at least in analogous form in favor of the defendant, which the Federal Court of Justice established in the decision "DNS - Block" (judgment of October 13, 2022, I ZR 111/21, openJur).

According to this, an access provider shall be liable in accordance with the provisions of the § Section 7 (4) sentence 1 of the German Telemedia Act (TMG) is merely subsidiary in relation to the operator of the website and also to the host provider. Since a DNS resolver does not have a closer connection to the illegal activity than an access provider, it is to be placed on an equal footing with the latter in the chain of subsidiarity.

Conversely, the efforts of the right holder to claim against the operator of the Internet site and the host provider must in turn be measured against the criterion of reasonableness for the right holder, so that the prosecution of the right is not contrary to European law requirements (Article 8 (3) of Directive 2001/29/EC on the harmonization of certain aspects of the laws of the Member States relating to the protection of intellectual property).

copyright and related rights in the information society) cannot be circumvented.

aa)

In this case, the plaintiff has sufficiently fulfilled its primary obligation to file a claim against the site operator. A serviceable address, for example in the form of a notice in the imprint of the disputed pages, is not recognizable in this respect, so that further judicial or extrajudicial action against this primary claimant is not promising.

bb)

In the "DNS Blocking" decision, the Federal Court of Justice considered it necessary that proceedings for interim legal protection for information, if necessary in the Federal Republic of Germany, should generally be conducted against a host provider with an undisputed registered office in the European Union. In individual cases, this can only be omitted if there is no prospect of success for reasons to be explained by the claimant.

However, this case is given here. The very fact that an address of the host provider in Vilnius, i.e. Lithuania and thus the EU, actually exists cannot be established. A possible address in the Ukraine does not lead to the primary obligation mentioned. Further delivery attempts than the delivery via a courier described by the plaintiff cannot be demanded, since there is nothing to indicate that any other possibility would be promising. In particular, it is not decisive whether the service is attempted in or out of court, since the correctness of the address in the EU is already not beyond doubt. Further requirements would restrict realistic legal protection possibilities of the right holder too much.

e)

The risk of repetition is indicated and not refuted.

III.

In the absence of an occurrence of conditions, no decision is to be made on the auxiliary request.

IV.

The subsidiary decisions are based on sections 92, 269, 709 ZPO and sections 286 et seq. BGB.

Dr. Werner  
Judge at the district court