Legal Regulations on Access Blocking and Regulatory Situation

As of May 2025

General Information on Access Blocking

From a technical perspective, websites are identified and accessed via IP addresses, which are (alpha)numeric identifiers. However, IP addresses are difficult for Internet users to remember and are not very user-friendly, making them impractical for daily use. Therefore, IP addresses are generally assigned to readable “domain names” such as “www.eco.de”. To access a website, either the IP address OR the domain can be entered into the browser’s address bar.

With access blocking, providers of Internet services that consists of the transmission in a communication network of information provided by a recipient or the provision of access to a communication network (access provider) can prevent their customers from accessing certain domains or IP addresses via their service. In this regard, there are several technical options:

- DNS blocking

A “Domain Name System” (DNS) is a kind of “virtual address book” that associates IP addresses and domain names. If an access provider sets up a DNS block for a domain, the connection between the domain and the corresponding IP address is disconnected from the provider’s DNS server. As a result, entering the domain in the browser’s address bar will no longer be accessed to the website. However, it continues to exist. The website can usually still be accessed via the IP address or through an alternative DNS provider.

- IP blocking

With IP blocking, the access provider blocks access to an IP address. Internet users are then generally no longer able to reach the desired website by entering either the domain name or the IP address in the browser’s address bar.

- URL blocking

With URL blocking, specific subpages of a website and consequently only parts of a domain are blocked or redirected. However, to implement URL blocking, an Internet access provider would need to analyse the content of the data traffic. The European Court of Justice (ECJ) has ruled declared filtering measures using URL blocking as disproportionate and incompatible with European fundamental rights in the “Scarlet” and “SABAM” decisions.

What speaks against access blocking?

In principle, takedown is the most effective solution for dealing with illegal content. To achieve the takedown of illegal content, there is usually contact with the content provider or the hosting service provider. If the content provider or the hosting service provider complies with the request for deletion, the corresponding objectionable content is no longer accessible to all Internet users.

With access blocking, on the other hand, a curtain is merely drawn in a metaphorical sense in front of the illegal content. The attempt is made to prevent Internet users from accessing the corresponding content by means of the block as an obstacle. However, access blocking is relatively easy to bypass – just as it is usually relatively easy to peek behind a curtain. Nevertheless, access blocking is often used by legislators and regulators to combat illegal Internet content, as this is at least intended to prevent less experienced Internet users from accessing illegal offerings.

In addition, both IP blocks and DNS blocks often lead to overblocking.

With DNS blocks, access to an entire domain is always prevented or redirected. This means that the entire domain and all of its content (including the legal ones) cannot be accessed.

Numerous websites or other online services often use the same IP address. If a shared IP address is blocked by the access provider, none of the websites or online services located behind this IP address can be accessed by Internet users. This often leads to a far-reaching “overblocking” of web offerings with legal content.

Foreword: General liability framework for providers under Articles 4 et seq. DSA

Before addressing the various national regulations that enable the access blocking under certain circumstances, it is important to clarify who can be held liable for the dissemination of illegal content, according to the rules of the Digital Services Act (DSA) – i.e. who can be held accountable for remedial measures. This sequence is important, as several national regulations refer to it either explicitly or implicitly.

The DSA collectively defines relevant providers in Article 3(g) of the DSA as “intermediary services”. These are then differentiated more precisely between “hosting”, “caching” and “mere conduit”. The latter two services can be designated or classified as access providers in the context of the DSA and the other regulations listed here.

Content providers also play a role in the liability framework, even though they are not explicitly defined in the DSA. They are those responsible for making content available, as they select it, for example as website operators or content uploaders.

Accordingly, efforts to combat illegal content must first be directed at them. If this is not successful, the next step is to contact the hosting provider. The

liability rules for hosting providers are regulated in Article 6 of the DSA. According to this, hosting providers are only liable for illegal content once they become aware of it and then fail to remove it without delay.

Only when measures against the hosting provider are also unsuccessful may the access provider be held accountable. The liability rules for providers of access services in the sense of "mere conduit" can be found in Article 4 of the DSA, while Article 5 of the DSA is relevant for providers of caching services.

Providers of "caching" services are not liable for the content stored on their servers, as long as they do not modify it and comply with the general rules. They are only liable if they become aware of the removal or blocking of the information stored on their servers from its original source, or if a judicial or administrative authority has ordered the removal or blocking and they nevertheless fail to remove this information promptly.

Access providers of "mere conduit" services, on the other hand, are not liable at all as long as they neither select the recipient nor the transmitted content or do not initiate the transmission of illegal content. However, Article 4(3) of the DSA allows EU Member States to establish national provisions that permit blocking orders against access providers – the legal basis for the following regulations. However, such blocking orders against access providers – especially those of "mere conduit" – may only be used as a last resort to prevent access to illegal content.

Regardless of this exception, providers of any kind are not generally obliged under Article 8 of the DSA to monitor the content transmitted or stored via their services and to check it for potential legal violations.

Legal basis for access blocking

Despite the limited effectiveness of access blocking and the fundamental subsidiarity of recourse to access providers under the DSA's liability framework, there are a number of regulations that allow for access blocking in various contexts.

- Access blocking for the protection of minors online

Legal basis/Where regulated: Section 20 (1) and (4) of the Interstate Treaty on the Protection of Minors in the Media (JMStV - German) in conjunction with Section 109 (1) sentence 2 and (3) of the Interstate Media Treaty (MStV - German)

Who is authorised/responsible: State media authorities (via the German Commission for the Protection of Minors in the Media (KJM))

Access blocking for the purpose of protecting minors online may be imposed by the state media authorities. The legal basis for this is Section 20 (1) and

(4) JMStV in conjunction with and with reference to Section 109 MStV (specifically relevant here is paragraph 1, sentence 2, as well as paragraph 3). According to this, the state media authorities are expressly permitted to order blocking as a measure against previously identified violations.

Blocking orders against access providers are legally classified as measures against third parties and are therefore subject to the strict principle of subsidiarity. Accordingly, attempts must first have been made unsuccessfully against both the content provider and then subsequently against the hosting provider with the demand for cessation or deletion.

This follows from the provisions of Section 109(3) MStV as well as from the liability framework for the dissemination of online content under the DSA explained in the preamble, according to which providers of access services are generally not initially liable for the dissemination of prohibited content. Additionally, Section 109(3) MStV refers to the provisions of the German Digital Services Act (DDG). According to this, a provider who is not liable under Article 4 DSA cannot be held liable for damages or reimbursement of enforcement and procedural costs (see the German-language Section 7(3) DDG).

Furthermore, according to Section 109(3) MStV, blocking by the access provider must be technically feasible and reasonable. Therefore, the responsible State Media Authority or the Commission for the Protection of Minors in the Media (KJM) must, within the framework of a blocking order, carry out a comprehensive balancing of interests related to the specific individual case, which takes into account multi-dimensional fundamental rights relationships.

This means the rights to protecting minors online must be weighed against the rights of the site against which the blocking order is issued. The effects on users, content providers, access providers and overall protecting minors online must be considered.

In recent years, the State Media Authorities have issued numerous cease-and-desist orders against providers of pornographic content, which have even been confirmed by the courts (see Germany's OVG NRW 13 B 1911/21). Accordingly, protecting minors online in Germany is weighted so heavily that foreign providers cannot invoke the country-of-origin principle and must comply with German regulations for offerings in Germany. However, as these cease-and-desist orders could not be successfully enforced against providers of pornographic content, blocking orders were ultimately issued against access providers based in Germany, following the liability regime.

Some access providers are resisting these blocking orders – now also with reference to the DSA. According to the DSA, the disputed pornographic platforms are considered very large online platforms, meaning that the EU should be responsible for enforcing measures, not the media authorities. However, the corresponding court proceedings have not yet been completed, so a corresponding ruling on jurisdiction is still pending.

So far, the blocking orders issued to date have quickly proven to be ineffective. Several providers of pornographic content have changed the domain names of their websites in response to the blocking orders, thus circumventing the blocks.

- Further planned access blocking or relating to protecting minors online

Legal basis/Where regulated: Article 16 et seq. CSAM Regulation Draft

Who is authorised/responsible: Coordinating authority

In addition to the existing regulations in the MStV, further regulations concerning access blocking are currently being planned. The CSAM Regulation proposed by the European Commission, titled “laying down rules to prevent and combat child sexual abuse”, contains special provisions in Articles 16 et seq. regarding blocking orders related to depictions of child sexual abuse. Since this is still only a draft and not yet applicable law, it is currently not possible to predict how the regulations will function in practice – provided they remain part of the regulation and eventually become applicable law.

- Access blocking in cases of intellectual property infringement, Section 8 DDG

Legal basis/Where regulated: Section 8 DDG (German)

Who is authorised/responsible: Intellectual property rights holders

Unlike in other areas of law, there is no competent state authority in copyright law that can impose blocking orders on access providers. Instead, Section 8 DDG enables the rights holders themselves to directly request such blocking. However, the requirements for such blocking are very high. This is because the liability structure under Articles 4 to 6 of the DAS must also be considered. Accordingly, blocking by an access provider may only be a last resort if the rights holders have exhausted all other remedies without success.

A ruling by Germany’s Federal Court of Justice (BGH) in 2022 (I ZR 111/21) shows how far they actually have to go to achieve this. Several publishers from Germany, the UK and the US had filed a lawsuit because their intellectual property was being offered illegally on several websites. They had requested that Deutsche Telekom block access to the websites without first taking action against the hosting provider in Sweden. The BGH ruled that, contrary to the publishers’ argument, action against the hosting provider would have been reasonable. Only when this approach does not lead to success is it appropriate to demand a block by access providers.

- Further access blocking in copyright law

Legal basis/Where regulated: *Sections 6, 7 of the Code of Conduct CUII (German)*

Who is authorised/responsible: Clearing Body for Copyright on the Internet (Clearingstelle Urheberrecht im Internet - CUII)

In copyright law, there is also a self-regulation initiative within the framework of which access blocking is implemented. Instead of an official supervisory authority, the Clearing Body for Copyright on the Internet (Clearingstelle Urheberrecht im Internet - CUII) handles these matters. This is an association of copyright holders, such as GEMA or the Games Association, and access providers such as Telekom. Together, they self-regulate and voluntarily take action against websites whose content infringes copyright. There is no explicit legal basis for this in the law; rather, the procedure is based on a code of conduct that the CUII has set for itself.

According to this code, a rights holder must submit an application to the CUII's Review Committee, which must be chaired by a former judge. This committee reviews the application, taking into account established case law, and either rejects the application or issues a recommendation for blocking. Before a recommendation can be implemented, the German Federal Network Agency (BNetzA) must review the decision. Only after its approval is the decision delivered to the access providers. These providers then implement the recommendation voluntarily, but Section 10 of the code of conduct explicitly allows them to file a complaint and take legal action against the decision if they have legal concerns.

Even though this CUII procedure is not explicitly regulated by law, it is nevertheless in line with applicable law. The provision in Section 8 DDG, which has already been cited several times, does not impose formal requirements, such as a judicial review of a blocking order. In this respect, there is no contradiction with the CUII procedure.

However, the CUII's approach has faced some criticism in the past, and court rulings in other cases could set important precedents for its work. In 2024, the CUII had to revoke some blocking recommendations after research by journalists revealed that several domains were no longer being used to commit copyright infringements and had been released for sale. Furthermore, in a legal dispute between a rights holder and the provider of a DNS resolver service, the Dresden Higher Regional Court ruled that the latter could not be held liable for copyright infringements as a disruptor under Section 8 DDG, let alone as an accomplice under Section 97 UrhG (see Dresden Higher Regional Court 14 U 503/23). This ruling is also in line with the liability privilege repeatedly mentioned several times and explained above in Article 4 DSA. Finally, the rights holder had not exhausted less intrusive alternatives, such as blocking via the hosting provider.

Even if the ruling does not directly declare the work of the CUII to be unlawful, it does show the enormous legal hurdles that must be overcome before such a block is actually legal.

- Access blocking in financial law

Legal basis/Where regulated: Section 37 I 1, 4 KWG (German)

Who is authorised/responsible: Federal Financial Supervisory Authority (BaFin)

Blocking orders are also possible in financial law. According to Section 37 (1) sentences 1 and 4 of the German Banking Act (Kreditwesengesetz, KWG), the German Federal Financial Supervisory Authority (BaFin) may demand the cessation of business operations if these violate certain specifications. According to sentence 4, BaFin may direct the necessary measures against companies involved in the initiation, conclusion or processing of such transaction. While the law does not explicitly mention blocking as a measure or access providers as addressees, there are more detailed interpretations through court rulings.

One access provider filed a lawsuit against BaFin at the Administrative Court in Frankfurt, which demanded that the website of a financial services provider in the Netherlands be blocked (see Administrative Court FFM 7 K 800/22). BaFin had investigated the service provider because it did not have the required authorisation for its business activities. In cooperation with the Dutch supervisory authority, BaFin had identified the service provider and requested it to cease operations, but without success. Subsequently, it demanded the blocking of the website.

The court confirmed that Section 37 KWG can in principle provide a legal basis for such blocking orders, as these are a possible measure for ceasing business operations. Furthermore, it can also be applied to access providers, which the court explicitly viewed as companies involved in processing according to Section 37 I 4 KWG. However, the court did not consider this measure to be proportionate in this case, as the authority had not exhausted all possibilities to have the website blocked by the hosting provider. Even if this alternative was no more promising than the blocking order against the access provider, the authority should have pursued this course of action. A blocking order against an access provider should only be the very last resort.

This argumentation of blocking by the access provider as the last resort aligns with the reasoning in the previously described copyright case and the liability framework under the DSA, even if the KWG does not expressly mention this. In financial law, too, a blocking order against access providers is therefore possible in theory, but in practice so difficult to achieve that it can hardly be reached with legal certainty

- Access blocking in gambling law

Legal basis/Where regulated: Section 9 I 3 No. 5 State Treaty on Gambling (GlüStV - German)

Who is authorised/responsible: Joint Gambling Authority of the Federal States (GGL)

Under gambling law, blocking orders may be issued by the Joint Gambling Authority of the German Federal States (GGL). The legal basis for this is Section 9 (1) sentence 3 No. 5 of the State Treaty on Gambling (GlüStV - German) in conjunction with the liability regulations originally contained in Sections 8 to 10 of the Telemedia Act (TMG), which have now incorporated into the DSA (see above). (Note: the wording of the GlüStV still refers to the TMG, which has been out of force since 2024 and replaced by the provisions of the DDG and DSA). This means that the GGL can also request access providers to block access to certain websites as long as the general requirements for the subsidiary liability of access providers are met.

In practice, however, this is not always clear, as case law shows (see OVG RP 6 A 10998/23). In this case, an access provider had sued against a blocking order issued by the GGL, which had demanded the blocking of several gambling websites based in Malta. The court ruled that the blocking order was unlawful. The regulation in Section 9(1)(3)(5) GlüStV was only applicable to service providers responsible under Sections 8 to 10 TMG (now: Articles 4 to 6 DSA). However, a mere provider of Internet access is not responsible for infringing acts committed via the Internet access it provides. An enforceable and court-backed blocking order against an access provider – at least according to the GlüStV – appears almost impossible in practice.

- Access blocking against Russian websites

Legal basis: Article 2f(1) of Regulation No. 833/2014, as amended by Article 1 of Regulation 2022/350, based on Article 215 TFEU

Who is authorised/responsible: EU Commission, state media authorities

Finally, there is a special case of access blocking – namely, blocking Russian content due to sanctions related to the war of aggression against Ukraine. Following the annexation of Crimea in 2014, the EU imposed sanctions against Russian companies under Regulation No. 833/2014, which it is authorised to do under Article 215 TFEU.

Following the attack on Ukraine in 2022, the EU adopted a new Regulation 2022/350, which supplemented the original Regulation with further sanctions. The newly inserted Article 2f prohibits operators from broadcasting or distributing the content of Russia Today Deutschland and Sputnik. This prohibition covers “transmission or distribution by any means, such as cable, satellite, IPTV, Internet service providers, Internet video sharing platforms or

applications, whether newly installed or pre-installed.” Accordingly, access providers are also covered by this prohibition.