SUBJECTIVE RIGHT TO ACCESS CONTENT ON THE INTERNET AS A PREREQUISITE FOR USING AI TOOLS

Jaroslav Kuba*

Abstract: *The paper examines the legal framework governing access to internet content as a prerequisite for the use and operation of generative AI tools. It highlights the technical foundations of internet connectivity, the role of ISPs, and the significance of network neutrality under EU Regulation 2015/2120, which establishes a subjective right to access and distribute online content. The analysis explores lawful exceptions to this principle, including measures under Czech and EU legislation that mandate content blocking for reasons such as gambling regulation, pharmaceutical safety, food protection, sanctions, and disinformation control. The study concludes that while the right to open internet access is fundamental, the growing number of legislative exceptions and their broad interpretation pose challenges to legal certainty and the practical availability of online content essential for AI technologies.*

Keywords: *Open Internet Access, Network Neutrality, Content Blocking, Generative Artificial Intelligence, Subjective Right to Access*

INTRODUCTION

Artificial intelligence has recently emerged as a topic that dominates discussions across a wide range of fields. Although the specific possibilities for the practical application of technologies labelled as such are still largely being explored, various tools of so-called generative artificial intelligence have already been available to the general public for some time, and in many forms. One of their common features is that they are operated on remote servers, and therefore only accessible to users online. Similarly, their machine learning methods are generally based on web scraping, whereby they collect relevant data freely accessible on the internet.

Therefore, the accessibility of internet content is a key precondition both for the use of most current generative AI tools and for their operation as such. This issue clearly has broader implications, since the internet is undoubtedly the dominant means of accessing information, multimedia, and communication in general today.

This raises a more general question concerning the legal framework governing the accessibility of content on the internet, as well as – from the reverse perspective – under which circumstances may it potentially be made inaccessible. The aim of the following text is to outline certain aspects of this issue to the esteemed reader.

* Mgr. Jaroslav Kuba, is a Ph.D. candidate at the Centre for Intellectual Property Law, Faculty of Law, Charles University, Prague, Czech Republic. ORCID: 0000-0002-5444-5430.
This paper was written as a part of the Specific University Research (SVV) project of Charles University No. 260748 "Challenges of Private Law: sustainability and technology."

I. TECHNICAL ASPECTS OF CONTENT DISTRIBUTION

At the outset, it must be acknowledged that such a broadly defined question offers an extensive range of perspectives, as the internet is by no means an isolated phenomenon; rather, a whole range of activities currently takes place predominantly, or even exclusively, within its environment. To narrow down the topic, it could be useful to begin by describing, in a highly simplified manner, how the internet actually functions and what basic categories of relationships can be identified within it.

In general, the internet can be defined as a worldwide, publicly accessible data network that interconnects end devices (endpoints) located in various geographical locations on Earth, enabling their data communication in the form of packet transmission, i.e., individually organised segments of data. From a closer perspective, the internet may be viewed as a system of interconnected networks[1] via individual nodes, which has the practical significance of not only providing multiple possible paths of connection between two given endpoints but, above all, giving the internet its decentralised character – which may be described as its primary defining feature. Communication occurs between any two or more devices connected to the internet such that each packet only carries its destination address (represented by the IP address, as explained below), without any fixed route between the nodes (or other points) of the network. As a consequence, even if part of the internet's infrastructure is taken out of operation, the possibility of communication through it generally remains preserved, ideally without any specific degradation of transmission quality (in a network-neutral approach, which will be addressed later). This implies that the Internet itself is very difficult to regulate by governments or other interest groups.

The actual Internet connectivity is provided by Internet Service Providers (commonly referred to by the abbreviation ISP). In a broader sense, which is more consistent with this English term, ISP refers to any entity that provides some internet infrastructure service - thus, in addition to connecting users to the internet, this also includes data transmission, or, for example, hosting services, i.e., providing data space on servers to other entities.

However, it is necessary to distinguish between the internet as such, and the services provided through it. There are numerous kinds of services, ranging from email, websites, search engines, news servers, e-shops, to social networks, or, for instance, generative AI tools. From a practical point of view, the provision of such services occurs in such a way that the data content constituting a given service is located on a server connected to the internet somewhere on Earth, while the user (the recipient of the service) accesses it using other elements of the Internet infrastructure remotely from where they or their device is located. This is fairly self-evident, but in order for someone to successfully access

[1] For example, BEREC understands the internet in its Guidelines on the Implementation of the Open Internet Access Regulation: *for the purposes of the Regulation, BEREC understands the term "Internet" to mean a global system of interconnected networks enabling connected end-users to connect with each other. An Internet access service enables such access to the Internet.* point 14. In: *BEREC* [online]. [2025-10-24]. Available at: <https://berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-of-the-open-internet-regulation-0>.

certain content on the internet (i.e., use a particular service or, more specifically, obtain certain information), it is necessary that such content is not only created and published by someone (meaning the respective service must actually be operated), but also the data communication between the server and the user needs to take place, therefore all ISPs involved must properly deliver their services, from hosting the content, through data transmission, to providing internet access to the user. Moreover, the availability or functionality of services may also in fact depend on other services, notably search engines, advertising or payment systems, etc.

It is apparent that not only the user and the provider of the content (service) themselves, but also particular ISPs or providers of the ancillary services may be located in different jurisdictions. Depending on the type of service, neither the user nor the provider of the given service may have any contractual relationship with these parties. Finally, the provider of a service may simultaneously provide internet infrastructure services (i.e., an ISP), which is particularly true of the largest players (e.g., Alphabet, the parent company of Google).

II. IP ADDRESSES AND DOMAIN NAMES

As already indicated, every device connected to the Internet is identified by a unique IP address assigned by the ISP. The technical details of how this mechanism works are beyond the scope of this article; however, it is essential to note that an IP address takes either a numerical or alphanumerical form (depending on the standard employed, e.g., 77.75.78.29 or 2a02:598:a::78:29). In order to avoid the necessity of entering the IP address of a server directly when accessing a particular service or content, the Domain Name System (DNS) was established. This system assigns of one or more symbolic names – domain names, such as *google.com*, to a specific IP address.

A particular domain name itself consists of several components in a hierarchical tree structure, ordered from the lowest to the highest level and separated by dots. This structure is also mirrored in the organisation of the administration of domain names. The highest level, which is always present in a domain name, is the TLD (Top Level Domain). In the example of the domain *google.com*, this is the *.com* section, followed by the second-level domain (*google*), and further levels may continue thereafter. Within a given level, each domain must be unique, although this does not apply when combined with different higher-level domains.

Generally, the highest domain level – which is not explicitly reflected in individual domain names – is the root domain, administered by the non-profit organisation ICANN (Internet Corporation for Assigned Names and Numbers). ICANN delegates the administration of individual top-level domains (such as .cz, .com, etc.) to other entities, the administrators of the respective domains.

The national administrator of the Czech ccTLD *.cz* is the association of legal entities CZ.NIC. The Czech national domain is decentralised, meaning it allows registration through independent registrars. By the example of the Czech national domain, the applicant (typically a provider of a particular service) registers a domain name by concluding a domain registration agreement with a registrar (which includes acceptance of the Rules

for the Registration of Domain Names in the ccTLD.cz), thereby becoming the holder of that domain name.

The mutual conversion of a text domain name to the (alpha)numerical form of an IP address is performed by the Domain Name System (DNS) through servers that translates the domain names to IP addresses. For the practical context of making content inaccessible, it is significant that there are various types of DNS servers – notably authoritative nameservers, which permanently store the original records within a domain zone, and recursive servers, which temporarily *mirror* records from authoritative servers. Their purpose is to provide users with faster response times and thus establish a connection to the requested server. These are typically operated by ISPs (a user's device will, in its default settings, generally connect to the DNS server of their internet service provider, although the use of any other DNS server could be set manually).

III. LAW AND THE INTERNET

In seeking an answer to the question of identifying the legal framework for the accessibility of content on the internet (and the lawful possibilities for restricting access to it), we may now identify two areas which, although interrelated, need to be considered separately from both a functional and a regulatory perspective: the actual provision of content in the sense of the operation of services accessible via the internet, and, on the other hand, the facilitation of the communication, i.e., access to these services through internet infrastructure. In this context, the perspective of *content inaccessibility* can be understood in two ways: either as the removal of content from its location within the network, or as any restriction that functionally prevents a user from obtaining the content (which itself has not been removed from its location, i.e., the server) in the usual manner. While it is unimportant for the ultimate consequence of the (in)accessibility of the content, by which of these two pathways it is achieved, the practical difference lies predominantly in whether the content in question is removed by the service provider itself, or whether access to it is effectively prevented by some other entity *along the way*. This article will therefore focus on analysing the latter option, which may thus be characterised as the availability or accessibility of content published on the internet.

Although the term *Internet* can be found in quite a considerable amount of legislation, it is not itself legally defined in any of them. Rather, statutes use in connection with the internet a number of different terms which have more or less different meanings depending on the particular legislative context. The provision of the Internet in the infrastructural sense falls primarily under the Act No. 127/2000 Sb., on Electronic Communications (ZoEK), which expressly excludes the content of services from its scope.[2] The internet by

[2] Section 1(2) ZoEK: *This Act does not apply to the content of services provided over electronic communications networks, such as the content of radio and television broadcasting, financial services and certain information society services, unless otherwise provided. The separation of transmission regulation from content regulation is without prejudice to the links that exist between them, in particular to guarantee media pluralism, cultural diversity and consumer protection.*

ZoEK is defined as one type of the *electronic communications network*.[3] Furthermore, this act defines 'the Internet access service'[4] as a type of 'electronic communications service', which is a service usually provided for remuneration through electronic communications networks. Provided that no one is excluded in advance from using such a service, it is a 'publicly available electronic communications service'.[5]

The Electronic Communications Act generally regulates the conditions for providing publicly available electronic communications services, including ensuring their security and integrity, confidentiality of communications, etc. The Act itself does not directly contain provisions that relate to making content inaccessible as such, although it does include rules that are relevant to this matter. The first of these is the exclusion of the provider's liability for the content of transmitted messages,[6] which, as already mentioned, is outside the scope of its regulation. Another is the obligation to provide publicly available electronic communications services continuously throughout the year, subject to quality-of-service requirements.[7]

In this context,[8] the Electronic Communications Act refers to the Regulation (EU) 2015/2120 of the European Parliament and of the Council on the Open Internet Access,[9] which governs the principle of network neutrality, central to the topic of this analysis. The term "network neutrality" represents the principle of equal treatment of data transmitted over the internet, meaning a prohibition on favouring or, conversely, restricting or blocking access to certain content by internet service providers, in relation to both content providers and users. Neutrality also applies to the pricing of data transmission – the content, type, source, or recipient of the data shall not be reasons for a different treatment.

According to the Regulation, both users and providers of content and applications[10] have the right to access and distribute their information and content, operate and provide applications and services, and use the terminal equipment of their choice, irrespective of the location of the end user or provider, or the location, origin or destination of the information,

[3] Section 2(2)(b) ZoEK: *Electronic communications network (means) transmission systems, whether or not they are based on permanent infrastructure or are centrally capacity-controlled, and, where applicable, connecting or routing equipment and other means, including inactive network elements, which enable the transmission of signals over lines, by radio, by wire, optical or other electromagnetic means, including satellite networks, fixed circuit or packet switched networks, including the Internet, mobile networks, power distribution networks to the extent that they are used for the transmission of signals, radio and television broadcasting networks and cable television networks, regardless of the type of information transmitted.*

[4] Section 2(3)(a)(1) ZoEK.

[5] Section 2(3)(e) ZoEK.

[6] Section 61(5) ZoEK.

[7] Section 61(1) ZoEK.

[8] Section 71(3) ZoEK.

[9] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union as amended.

[10] See ECJ C-807/18 and C-39/19 Telenor Magyarország, paragraphs 36–38. According to the BEREC Guidelines, content and application providers are protected as end-users under the Regulation when content and application providers use an Internet access service to reach other end-users.

content, application, or service, through their internet access service.[11] In other words, the Regulation establishes a **subjective right of access to content distributed on the internet**.

Internet access service providers have a corresponding 'general obligation of equal treatment',[12] i.e., an obligation to treat all traffic equally when providing internet access services, without discrimination, restrictions or interference, and without regard to the sender and recipient, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used,[13] and must not implement traffic management measures that exceed this framework.

Significantly, the Regulation explicitly prohibits providers from blocking, slowing down, altering, restricting, interfering with, degrading or discriminating specific content, applications or services or specific categories thereof, as well as from implementing any other measures going beyond reasonable traffic management. However, the Regulation allows three exceptions, which may be applied where necessary and only for as long as strictly required. Two of these are aimed at maintaining the integrity and security of the network, or preventing its imminent overload, thereby permitting interventions essentially of a technical nature, such as in the case of cyberattacks.

The final, and in practice the most important exception, allows for measures (including blocking of content) to be taken in order to *'comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers'*.[14]

IV. BLOCKING OF CONTENT ON THE INTERNET

We may now proceed to examine specific legal provisions which make use of the above exceptions to the prohibition on making content inaccessible at the level of communication through internet infrastructure, and which therefore constitute lawful restrictions on the subjective right to access content on the internet in the Czech Republic. In this context, it may be noted that the number of such regulations is increasing. From a historical perspective, it is noteworthy that at the time of the adoption of the first such measure (not very long ago, in 2016), a relatively widespread wave of criticism emerged, pointing not only to the risk of censorship of the internet as such, but also to the concern that it might soon be followed by numerous further measures.[15]

---

[11] Article 2(2) defines an *'Internet access service'* as an electronic communications service that provides access to the Internet and thus connectivity to virtually all Internet endpoints, regardless of the network technology and terminal equipment used.

[12] See ECJ C-854/19 Vodafone (roaming), paragraph 26; C-5/20 Vodafone (tethering), paragraph 25 and C-34/20 Telekom Deutschland (throttling), paragraph 28.

[13] In the Czech context, these are electronic communications entrepreneurs offering and providing a publicly available internet access service. In: *Czech Telecommunication Office* [online]. [2025-10-24]. Available at: <https://ctu.gov.cz/otevreny-internet-pravidla-sitove-neutrality>.

[14] Article 3(3)(a) of the Regulation (EU) 2015/2120 on the Open Internet Access.

[15] In: *root.cz* [online]. [2025-10-24]. Available at: <https://www.root.cz/clanky/zakon-o-cenzure-muze-byt-v-rozporu-s-ustavou-hlasovat-se-bude-ve-stredu/>.

This first regulation was included in the Act No. 186/2016 Sb. on Gambling, under which *'the internet access service provider pursuant to the Electronic Communications Act is required to prevent access to a website listed on the list of unauthorised internet games'*.[16] This register, containing the URL addresses (domain names) of such sites, is maintained by the Ministry of Finance, which ex officio enters and deletes records therein. Under the wording of the amendment effective from the beginning of 2024, the register now includes not only websites through which prohibited online gambling is operated, but also websites which *'substantial purpose is to cause, enable, facilitate or conceal the breach of the prohibition on operating of a prohibited internet game'*.

Apart from the general objections already mentioned, this act has also been criticised specifically for its vagueness in defining the obliged entities, the terminology used (notably the term "website"), and the manner in which blocking was to be implemented. However, the Constitutional Court found the act to be in conformity with the constitutional order, both in the mentioned as well as more general respects (particularly towards the alleged interference with the freedom of expression and the right to information under Article 17 of the Charter of Fundamental Rights and Freedoms).[17] The Ministry of Finance has also issued a methodological guidance,[18] which specifies in more detail how the blocking shall be carried out. Specifically, the Ministry recommends blocking through the DNS servers of internet service providers, which is indeed the method actually employed.[19] As described above, this means that a user using the DNS server of a Czech ISP provider will not be connected to the requested website upon entering the relevant address. Such a method is not particularly difficult for users to circumvent; however, according to the Ministry, this is sufficient for the provider to meet its obligation.

The next legislation at the national level making use of the exceptions under the Regulation is Act No. 378/2007 Sb., on Pharmaceuticals. Blocking under this act is structured in essentially the same way as under the Gambling Act. This legislation establishes two lists. One of them is a register of sites offering pharmaceutical products illegally, maintained by the State Institute for Drug Control (SÚKL), and the other is a register of sites offering veterinary medicines illegally, maintained by the Veterinary Institute. In both cases, an internet access provider within the Czech Republic is again required to prevent access to the websites listed in the respective register. In practice, providers fulfil this obligation in a similar manner to that used for gambling sites, i.e., through DNS servers.

Essentially the same may be said about the most recent of these registers, which is the list of websites offering dangerous foods, maintained by the State Agricultural and Food Inspection Authority pursuant of the act of the same name.[20] Across all four registers there are currently dozens of records.

---

[16] Section 84a of Act No. 186/2016 Sb. on Gambling.

[17] Ruling of the Constitutional Court of 14 February 2017, Case No. Pl. ÚS 28/16 in the case of a proposal to repeal certain provisions of Act No. 186/2016 Sb. on Gambling.

[18] Methodological Instruction of Department 34 - State Supervision of Gambling.

[19] In: *cesnet* [online]. [2025-10-24]. Available at: <https://www.cesnet.cz/2017/07/jak-blokujeme-nepovolene-hazardni-weby/>.

[20] Section 3d of Act No. 146/2002 Sb., on the State Agricultural and Food Inspection and on amendments to certain related acts.

In connection with the conflict in Ukraine, the Council of the European Union issued Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, as amended, which in 2022 prohibited *'operators to broadcast or to enable, facilitate or otherwise contribute to broadcast, any content by the legal persons, entities or bodies listed in Annex XV, including through transmission or distribution by any means such as cable, satellite, IP-TV, internet service providers, internet video-sharing platforms or applications, whether new or pre-installed.'*[21]

This annex lists the names of television stations, mostly from the Russia Today and Sputnik family. Although the language implies that these stations should be prevented from their broadcasting, in practice, in accordance with BEREC's opinion,[22] the entire websites of the respective organisations are blocked, even if they contain content other than broadcasts or recordings of broadcasts of these channels (for example, the content of rt.com can be characterised as a news portal). This duty is again implemented by ISPs at the level of DNS servers.

Finally, the last legal instrument under which content blocking is implemented pursuant to the mentioned exception of the Regulation is Act No. 69/2006 Sb., on the Implementation of International Sanctions. Specifically, it concerns the restriction or prohibition of the provision of electronic communications services for the purpose of communication with an entity or person subject to international sanctions or providing other connections to such an entity or person if they are listed in a sanctions list under this act.[23]

Regarding the national case law, it is worth noting the ongoing proceedings concerning the blocking of a group of websites designated by the government in February 2022 as disinformation sites. Among others, certain ISPs proceeded to block these sites based on non-binding instructions or requests they received from the government and some other authorities. This approach was subsequently challenged in court, which at second instance (as of spring 2025) found that such blocking of content access on the internet without a legally relevant ground that would qualify for the exception under the Regulation is illegal.[24]

In this context, it is also worth mentioning that on the basis of these informal instructions, the domains of the websites in question were blocked by the administrator

---

[21] Article 2f of Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's activities destabilising the situation in Ukraine, as amended.

[22] In: *BEREC* [online]. [2025-10-24]. Available at: <https://www.berec.europa.eu/en/news-publications/news-and-newsletters/berec-supports-isps-in-implementing-the-eu-sanctions-to-block-rt-and-sputnik>.

[23] Section 6(2)(b) and (c) of Act No. 69/2006 Sb. on the implementation of international sanctions.

[24] Resolution of the Municipal Court in Prague of 29 February 2024, Case No. 20 Co 6/2024, paragraph 9: *'If the defendant claims that any of the above-described exceptions to the prohibition of blocking was applicable in the applicant's case, they must substantiate and prove such a fact with respect to the applicant in a very specific manner. The defendant, as a multinational company with trained managers and lawyers, cannot successfully argue that it was in error or in good faith as to the binding nature of the NCKO's request, since it must have been clear from its wording as a request for cooperation that it was not a binding decision of the State administration ordering the providers to carry out the requested blocking, and that the NCKO, as part of the military intelligence service, had no authority in that regard. Even less could they have considered that they were bound to take the action in question by a very general and vague government resolution.'*

CZ.NIC.[25] However, it must be pointed out that not every ISP in the broader sense (such as domain administrators) falls under the definition of an internet access services provider within the meaning of the Regulation. This creates a rather extensive *grey area* the existence of which the operators of these websites have involuntarily experienced.

Another dimension of the matter is the liability of ISPs as providers of information society services for the content they transmit or host, but this already brings us to the area of making content inaccessible in the sense of its actual removal, which is beyond the scope of this article. For the sake of completeness, it may be noted that, irrespective of the nature of the content, the provider is not liable in cases of mere transmission or caching, provided that the conditions of the so-called safe harbour mechanism are met, which is currently governed by the DSA Regulation.[26]

CONCLUSION

As outlined in the introduction, the issue of making content inaccessible on the internet is a very complex topic, which is of great importance as a prerequisite for the use of AI tools. It may be summarised that at the level of communication via internet infrastructure, the availability of content as a subjective right (both in terms of access by users and distribution by content providers) is established by the Open Internet Access Regulation, including corresponding obligations for providers of Internet access services not to obstruct it.

The Regulation allows only strictly defined exceptions from this principle, which are, however, applied in a relatively flexible manner. Although they should only block access to content for a strictly necessary period of time, in reality this period of time tends to be indefinite, and the legal grounds for blocking are in some cases based on an interpretation that may be somewhat questionable. In this context, it cannot go unnoticed that although the legal basis is generally legislative, the determination of the specific services to be blocked is usually delegated to executive bodies. Meanwhile, the amount of *blocking* legislation is clearly on an upward trajectory.

[25] In: *nic.cz* [online]. [2025-10-24]. Available at: <https://www.nic.cz/page/4317/sdruzeni-cznic-vyzvalo-vladu-ke-koncepcnimu-reseni-problemu-dezinformacnich-domen/>.

[26] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act).