**LIDC Vienna 2025**

**Report of the Hungarian Competition Law Association**

**HUNGARY**

**Question B: What responsibility or obligations should online platforms have when it comes to eliminating infringements by their users, especially in the areas of IP and unfair competition?**

*International Rapporteur: Univ.-Prof. Dr. Nikolaus Forgó, Professor of Technology Law and IP Law, Head of the Department for Innovation and Digitalisation in Law, University of Vienna, Austria*

*Hungarian National Rapporteurs:*

*Bálint HALÁSZ (Balint.Halasz@twobirds.com), Ádám LIBER (Adam.Liber@Liber.hu)*

*Members of the Working Committee:*

*Mihály BUDAI, Eszter FODOR, András GAÁL, Zsolt GYEBROVSZKI, Bálint HALÁSZ, Ádám LIBER, Fanni OROSZI, Kenéz SZABÓ, István SZATMÁRY, Szabolcs STOCK, Péter VIRÁG.*

This Hungarian country report provides an analysis of the legal framework governing the liability and responsibility of online platforms in Hungary, with a specific focus on infringements of intellectual property rights and unfair competition. The Hungarian legal landscape has undergone a significant transformation, moving from a system based on the domestic implementation of the EU's E-Commerce Directive (ECD) to one directly governed by the Digital Services Act (DSA). This shift has introduced new obligations, refined existing principles, and established a new institutional framework for enforcement.

We examine the historical evolution of platform liability, the current legal bases for civil and criminal responsibility, specific obligations related to content monitoring and reporting mechanisms, and the crucial interplay between the enforcement of intellectual property rights and the protection of fundamental rights. It draws upon Hungarian national legislation, EU regulations, administrative practice from key authorities such as the Hungarian Competition Authority (HCA) and the National Media and Infocommunications Authority (NMHH), and relevant national and European case law.

**Abbreviations:**

|  |  |
| --- | --- |
| Advertising Act | Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities |
| APA | Act CXL of 2004 on the General Rules of Administrative Procedures and Services |
| Civil Code | Act IV of 2013 on the Civil Code |
| Code of Civil Procedure | Act CXXX of 2016 on the Code of Civil Procedure |
| Competition Act | Act LVII of 1996 on the Prohibition of Unfair and Restrictive Market Practices |
| Copyright Act | Act LXXVI of 1999 on Copyright |
| Criminal Code | Act C of 2012 on the Criminal Code |
| DSA | Digital Services Act, Regulation (EU) 2022/2065 |
| ECD | EU E-Commerce Directive (Directive 2000/31/EC) |
| E-Commerce Act | Act CVIII of 2001 on Electronic Commerce and Information Society Services |
| HCA | Hungarian Competition Authority (*Gazdasági Versenyhivatal*) |
| HIPO | Hungarian Intellectual Property Office |
| Kúria | Hungarian Kúria (formerly Supreme Court) |
| NMHH | Hungarian National Media and Info-communication Authority |
| OCSSP | Online Content-Sharing Service Provider |
| OPVT | Online Platform Dispute Settlement Council (*Online Platform Vitarendező Tanács*) |
| Patent Act | Act XXXIII of 1995 on the Patent Protection of Inventions |
| Trademark Act | Act XI of 1997 on the Protection of Trademarks and Geographical Indications |
| UCP Act | Act XLVII of 2008 on the Prohibition of Unfair Business-to-Consumer Commercial Practices |

**Historical perspective**

1. **Substantive (legal) developments**

For over two decades, the legal regime governing platform (i.e., online intermediary) liability in Hungary was based on the European E-Commerce Directive (Directive 2000/31/EC, hereinafter **ECD**) and its domestic implementation via the Act CVIII of 2001 on Electronic Commerce and Information Society Services (hereinafter: **E-Commerce Act**). This framework established conditional[[1]](#footnote-1) liability exemptions, or “safe harbours,” for intermediary service providers engaged in mere conduit, caching, and hosting activities, alongside a general prohibition on imposing monitoring obligations[[2]](#footnote-2). These exemptions were central in delineating the responsibilities of content providers, who are primarily liable for the information they create, from those of intermediaries, whose role is typically technical and passive. The E-Commerce Act confirmed in its former Section 12 that if a user of the service is acting under the authority or control of the intermediary, then the safe harbour does not apply. Thus, an intermediary that colludes with users in unlawful acts, or knowingly solicits illegal content, would lose immunity.

The transition to the Digital Services Act (**DSA**), which became fully applicable on 17 February 2024, marks the most significant development. As an EU Regulation, the DSA's provisions on liability exemptions (Articles 4-6) are directly applicable in Hungary, achieving full harmonization in this area and substantively updating the legal framework.

* 1. **The definition of platforms or similar**

Under the pre-DSA regime, the E-Commerce Act defined[[3]](#footnote-3) an “intermediary service provider” functionally, based on the activities of mere conduit, caching, hosting, and, notably, search engine services (termed “location tool services”). The term “platform” was not explicitly defined but was understood to fall under the hosting category.

The DSA introduces a more structured hierarchy. It defines “intermediary services” as mere conduit, caching, and hosting services. A subset of hosting services is defined as “online platforms,” which are services that not only store information but also disseminate it to the public at the request of a user (e.g., social networks, online marketplaces). The DSA further distinguishes “Very Large Online Platforms” (VLOPs) and “Very Large Online Search Engines” (VLOSEs) based on user thresholds, subjecting them to more stringent obligations. Following the DSA's entry into force, the Hungarian E-Commerce Act was amended to simply refer to the DSA's definitions for intermediary services, thus fully aligning with the EU's terminology.

* 1. **International legal provisions**

The primary international legal provisions shaping Hungarian law have been those of the European Union. The ECD provided the foundational principles for over 20 years. Its key tenets—the country-of-origin principle, the prohibition of general monitoring, and the conditional liability exemptions for intermediaries—were transposed into Hungarian law.

As of 17 February 2024, the DSA has superseded the ECD's liability framework. Its provisions are directly applicable, ensuring a harmonized approach to intermediary liability exemptions across the EU, including Hungary. Other crucial EU instruments include the Copyright in the Digital Single Market (CDSM) Directive, whose Article 17 establishes a specific, stricter liability regime for Online Content-Sharing Service Providers (OCSSPs), and the Unfair Commercial Practices Directive, which underpins Hungarian consumer protection law.

* 1. **National legal provisions**

The cornerstone of national legislation has been the E-Commerce Act. This Act transposed the ECD and, for many years, detailed the conditions for safe harbour exemptions. While the DSA's liability rules are now directly applicable, the E-Commerce Act remains relevant. It has been amended to integrate the DSA, for instance by referring to the DSA's definitions and by establishing a specific national notice-and-takedown (NTD) procedure for certain intellectual property infringements.

Other key national laws include:

* *Act V of 2013 on the Civil Code (****Civil Code****):* Provides the general rules for contractual and non-contractual (delictual) liability.
* *Act C of 2012 on the Criminal Code (****Criminal Code****)*: Defines criminal liability, including for parties who abet or are accomplices to a crime.
* *Act XLVII of 2008 on the Prohibition of Unfair Business-to-Consumer Commercial Practices (****UCP Act****)*: Transposes the EU's UCPD and is the primary tool for combating unfair competition against consumers.
* *Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (****Advertising Act****):* Contains specific liability exemptions for publishers of advertising who act as neutral intermediaries.
* *Act LXXVI of 1999 on Copyright (****Copyright Act****)*: Implements the CDSM Directive, including the specific liability regime for OCSSPs in its Sections 57/A-H.
* *Act CIV of 2023 on Certain Rules regarding Internet Intermediary Services*: The Hungarian DSA Implementation Act, which designates the NMHH as the Digital Services Coordinator and establishes national enforcement procedures.
  1. **Cases**

Hungarian case law has evolved, often influenced by European jurisprudence. An early key decision from the Metropolitan Court of Appeal (No. 2.Pf.21.991/2009/5) established that an online forum operator, acting as a hosting provider, could not be expected to pre-screen all user comments, underscoring the principle of passive intermediation.

A landmark case that highlights a significant practical challenge is the Kúria's decision BH 2017.1.20. In this case, the Supreme Court ruled that an internet service provider could not be compelled in a civil copyright infringement proceeding to disclose the personal data of users associated with IP addresses, prioritizing data protection over the rightsholder's need to identify the infringer. This has created a persistent obstacle to effective IP enforcement against anonymous online infringers.

Cases from the European Court of Human Rights (ECtHR) have also been highly influential. In Magyar Tartalomszolgáltatók Egyesülete (MTE) and Index.hu Zrt v. Hungary[[4]](#footnote-4), the ECtHR found that imposing strict liability on a news portal for user comments that were offensive but not hate speech was a disproportionate restriction on freedom of expression. This decision clarified the scope of the earlier Delfi AS v. Estonia judgment, suggesting a tiered approach to platform responsibility based on the severity of the content. Similarly, in Magyar Jeti Zrt v. Hungary[[5]](#footnote-5), the ECtHR ruled that holding a publisher liable for merely hyperlinking to defamatory content was a violation of Article 10 of the European Convention on Human Rights (“**ECHR**”), as it failed to distinguish between dissemination and referencing. These cases have forced Hungarian courts to adopt a more nuanced balancing of competing fundamental rights in the digital sphere.

* 1. **Activities of platforms**

The legal framework distinguishes liability based on the platform's function. Platforms often have dual roles, acting as content providers for their own services (for which they are directly liable) and as intermediaries for third-party content (where they may be exempt). The key activities recognized in law are “mere conduit” (transmission), “caching” (temporary storage for efficiency), and “hosting” (storage at a user's request). The DSA now formally categorizes platforms that disseminate user content to the public, such as social media or online marketplaces, as a specific type of hosting service with additional obligations.

* 1. **Others (e.g. NGOs, stakeholders)**

The primary state stakeholder in the regulation of online platforms is the National Media and Infocommunications Authority (NMHH). Designated as Hungary's Digital Services Coordinator, the NMHH is responsible for supervising compliance with the DSA. It also operates the “Internet Hotline,” a reporting service that now functions as Hungary's first official “trusted flagger” under the DSA. The Hungarian Competition Authority (HCA) is the key stakeholder in enforcing unfair competition and consumer protection rules, frequently interacting with platforms to obtain information or compel the removal of unfair commercial practices.

Furthermore, the Online Platform Dispute Settlement Council (in Hungarian: Online Platform Vitarendező Tanács, Hungarian abbreviation: OPVT), the out-of-court dispute resolution body established in Hungary pursuant to Article 21 DSA will play a pivotal role in defining the practical contours of platform responsibility.

**Legal Basis for Liability and Responsibility**

1. **Legal basis for liability and responsibility of platforms**

The legal framework for platform liability in Hungary is built on a foundational principle derived from the ECD and now enshrined in the DSA: primary responsibility for illegal content lies with the user or entity that created it (the “content provider”).[[6]](#footnote-6) Intermediary service providers are subject to a fault-based liability regime where they are, in principle, liable for infringements committed via their services but benefit from broad, horizontal liability exemptions—or safe harbours—provided their role remains purely technical, automatic, and passive. These exemptions apply across civil, criminal, and administrative law, but do not prevent courts from issuing injunctions to terminate or prevent an infringement.

* 1. **Types of platforms**

Liability is determined by function, not by the platform's self-description. The law distinguishes between the online intermediary categories below:

1. **Mere conduit** is defined as “*consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network*”.[[7]](#footnote-7) This provider is not liable for the information transmitted or accessed by it if it does not (i) initiate the transmission; (ii) select the receiver of the transmission; and (iii) select or modify the information contained in the transmission.[[8]](#footnote-8)
2. **Caching** is defined as “*consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients upon their request*”.[[9]](#footnote-9) The caching provider is not liable for the storage of the information if it (i) does not modify the information; (ii) complies with conditions on access to the information; (iii) complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry; (iv) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and (v) removes or disables access to the information expeditiously upon obtaining actual knowledge that the information at the initial source was been removed from the network, access to it was disabled, or such removal or disablement was ordered by a court or administrative authority.[[10]](#footnote-10)
3. **Hosting** is defined as “*consisting of the storage of information provided by, and at the request of, a recipient of the service*”.[[11]](#footnote-11) The hosting provider is not liable for the storage of the information if: (i) it did not have actual knowledge of illegal activity or illegal content and, regarding claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (ii) upon obtaining such knowledge or awareness, removes or disables access to the illegal content expeditiously. Nevertheless, these exemptions do not apply and the hosting service provider therefore remains liable if (A) the recipient acts under the authority or the control of the provider; and/or (B) the provider allows consumers to conclude distance contracts with traders, and the platform presents the information or otherwise enables the specific transaction in a way that would lead an average consumer to believe that the information, product or service is provided either by the platform or by a recipient acting under its authority or control.[[12]](#footnote-12) This is the most relevant category for online platforms like social media, forums, and marketplaces. Their exemption depends on not having “actual knowledge” of the illegal content and, upon gaining such knowledge, acting expeditiously to remove or disable access to it. Under the DSA[[13]](#footnote-13), this exemption is lost if an online marketplace presents a third-party trader's offer in a way that misleads an average consumer into believing the product is sold by the platform itself.
4. Lastly, an **online search engine service** “*means an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found*”.[[14]](#footnote-14) While the DSA defines them separately, Hungarian law has historically treated them similarly to hosting providers, granting an exemption conditional on a lack of knowledge and prompt action upon notification. Online search engine providers are not liable for the damage caused with the publication of such information if: (i) it does not have knowledge of unlawful activity related to the information or that the information infringes the right or legitimate interest of any party; or (ii) upon obtaining such knowledge, it removes the information or disables access to it expeditiously.
   1. **Civil and criminal law**

As for **civil liability**, the provisions of Act V of 2013 on the Civil Code (“**Civil Code**”) apply. Under the Civil Code, civil liability may be either contractual or extra-contractual (delictual). In the first case, the provider is generally liable if it breaches the contract with the recipient and thereby causes damage to the recipient.[[15]](#footnote-15) In the second case, the provider is generally liable if it causes damage to the other party.[[16]](#footnote-16) Beyond the Civil Code, the DSA stipulates that if the provider infringes the DSA and the recipient thereby suffers damage or loss, the recipient is entitled to compensation,[[17]](#footnote-17) in which case the rules of contractual liability apply.[[18]](#footnote-18) Moreover, the Internet Intermediaries Act stipulates that the recipient may bring civil proceedings against the provider to resolve any dispute related to the service. Exceptionally, if the provider is established in another EU member state, the recipient is a consumer, and the parties did not agree otherwise, the recipient may bring civil proceedings before the court of their domicile for the breach of their right or legitimate interest related to the contract.[[19]](#footnote-19)

By contrast, there are no sector-specific rules for **criminal liability** for intermediaries. Act C of 2012 on the Criminal Code (“**Criminal Code**”) defines a “crime” as conduct which is (i) carried out intentionally or, provided that negligence is also punishable by the Criminal Code, by negligence, (ii) dangerous to society; and (iii) punishable under the Criminal Code. In turn, a conduct is “dangerous to society” if it breaches or threatens the person or rights of others, or the societal, economic or state order of Hungary, as defined in the Fundamental Law. Parties to a crime include the perpetrator, the indirect perpetrator, the co-actor (together: parties to a crime), the abettor, and the accomplices (together: conspirators). A perpetrator is a person who actually commits a criminal act, whereas an indirect perpetrator is a person who commits a wilful criminal act by using another person as an instrument whose punishability is excluded through infancy, insanity, constraint, menace, or error. Co-actors are persons engaged in a wilful criminal act jointly, having knowledge of each other’s activities. Lastly, the abettor is a person who intentionally persuades another person to commit a crime, while the accomplice intentionally helps another person commit a crime.[[20]](#footnote-20) In practice, the perpetrator could be the content provider/creator of the information, in which case the provider could act as a co-actor or conspirator. A hosting provider or an online search engine provider could also be considered a co-actor or an indirect perpetrator, provided that the provider commissioned or instructed the recipient to commit the crime.

* 1. **Direct and accessorial liability**

Hungarian law does not draw a sharp, formal distinction between direct and accessory liability in the context of online platforms. Instead, the analysis focuses on the nature of the provider's involvement. If the provider's role is purely technical and passive, it is considered an intermediary and benefits from the safe harbour exemptions. If the provider becomes “active”—for instance, by curating, promoting, or having knowledge and control over the illegal content without taking action—it loses the exemption and can be held liable as if it were the content provider. This functional approach effectively determines whether liability attaches, rendering a separate doctrine of “accessory” liability largely redundant. The key question is whether the platform has crossed the line from a neutral intermediary to an active participant in the dissemination of the content.

In the realm of **unfair commercial practices** and **advertising**, this principle is codified. The Advertising Act explicitly exempts[[21]](#footnote-21) a “publisher of advertising” from liability for an ad's content if the publisher qualifies as an intermediary under the E-Commerce Act and meets the safe harbour conditions. In effect, an online platform that merely carries someone else’s advertisement or product listing will not be held liable for false or illegal claims in that content, provided it functions neutrally (for example, an ad hosting service that does not materially modify ads and removes unlawful ads when notified). If the intermediary does go beyond a neutral role – say, if it had the ability and duty to review the content and failed to reject an obviously illegal advertisement – then general rules could impose liability, but even then Hungarian law gives an extra layer of protection. For instance, a publisher that simply disseminates ads to the public is generally not liable for the truthfulness of those ads (unless it had knowledge and a specific obligation to act). Hungarian authorities have mostly treated online platforms as “middlemen” not directly accountable for unfair business practices. The HCA has confirmed that these specific intermediary rules act as *lex specialis*, overriding any general liability that might otherwise be inferred from consumer protection law. [[22]](#footnote-22) In practice, this means platforms are not held liable for their users' unfair practices but are treated as essential partners in enforcement, with legal obligations to cooperate with HCA investigations and comply with orders to provide information or remove content. If a sanctioned business fails to stop an unfair practice (for example, a merchant keeps posting deceptive ads even after an order to cease), Hungarian law even allows authorities, in special cases, to require an “outside contractor” – which could be the platform hosting the content – to execute the order and remove the offending content themselves. This is a remedy of last resort, ensuring that the intermediary can be compelled to takedown illegal content if the direct violator refuses to comply. Non-cooperative intermediaries also face sanctions: under the Competition Act, failure to obey the HCA’s order (such as a demand to provide information) can lead to fines up to 1% of the company’s annual turnover. Thus, while not usually a principal offender, a platform in Hungary cannot simply turn a blind eye to unlawful activity on its service once alerted – it is expected to assist authorities and rightsholders by removing content and providing evidence when lawfully requested.

1. **Content monitoring requirements for Intellectual Property**

Generally, platforms are not required to monitor content generated by their users for possible infringements of intellectual property rights in Hungary. Article 8 of the DSA, which is directly applicable, codifies the long-standing principle from the ECD that intermediary service providers cannot be subjected to a general obligation to monitor the information they transmit or store, nor can they be required to actively seek facts indicating illegal activity. This prohibition on imposing general monitoring obligations on intermediary service providers was previously set out in Article 15 of the E-Commerce Directive, and Section 7 (3) of the E-Commerce Act and has been essentially retained without change in Article 8 of the DSA. The relevant provisions of the regulation are justified not only by the practical infeasibility of general monitoring but also by the fact that implementing a filtering system would effectively result in internet censorship and would unnecessarily and disproportionately infringe users’ rights to privacy and data protection. However, this prohibition only applies to general obligations, and does not affect the imposition of specific monitoring obligations in individual cases. It is also important to note that the liability exemptions for intermediary service providers do not preclude the issuance of judicial or administrative orders (including interim measures) aimed at terminating or preventing infringements, such as removing or disabling access to illegal data.

* 1. **Liability privileges available to platforms for IP infringements by their users**

Under the DSA, significant liability privileges are available for online intermediaries. The core protection comes from the safe harbour exemptions provided in Articles 4, 5, and 6 of the DSA for mere conduit, caching, and hosting services, respectively. These exemptions are horizontal, meaning they apply to liability arising from any type of law, including IP law. A platform that meets the conditions of these safe harbours is shielded from liability for damages or fines related to IP infringements committed by its users.

Furthermore, Hungary has a specific, highly formalized notice-and-takedown (NTD) procedure under the E-Commerce Act for copyright and trademark infringements. A platform that diligently follows the steps of this procedure – receiving a valid notice, taking down the content within 12 hours, notifying the user, and handling any counter-notice – is explicitly immunized from liability for the infringement in question.

A critical exception to these general privileges is the specific liability regime for Online Content-Sharing Service Providers (OCSSPs) under Article 17 of the CDSM Directive, implemented in the Hungarian Copyright Act and which takes precedence over the general DSA rules. This regime, implemented in Hungary via Sections 57/A-H of the Copyright Act, imposes stricter obligations on qualifying platforms, including making “best efforts” to obtain licenses and prevent the availability of specific infringing works based on rightsholder information (often involving content filtering). For other IP rights (like trademarks) or platforms not qualifying as OCSSPs, the standard DSA notice-and-action rules apply.

* 1. **Proactive monitoring and the “Good Samaritan” rule**

Platforms are allowed and encouraged to proactively monitor and remove user content without losing their liability privileges. This principle, often called the “Good Samaritan” rule, is explicitly established in Article 7 of the DSA. This provision was a crucial innovation, as the pre-DSA framework created a perverse incentive: platforms that voluntarily monitored content risked being deemed to have “actual knowledge” of illegal material, thereby losing their safe harbour protection. Under the ECD, liability exemptions applied only to activities that were of a mere technical, automatic, and passive nature, and voluntary investigations risked undermining these protections by implying that the provider had knowledge of the illegal content and thus could be held liable. This discouraged proactive content moderation.

Article 7 of the DSA resolves this by stating that an intermediary shall not be considered ineligible for liability exemptions solely because it undertakes voluntary, own-initiative investigations to detect and remove illegal content. This provision is significant because, while general monitoring obligations and proactive measures concerning illegal content cannot be mandated, it ensures that intermediary service providers do not lose immunity under the DSA for taking voluntary, good faith, and diligent actions to detect, identify, and remove illegal content or disable access thereto. For these actions to be protected, they must be conducted in good faith and with due diligence. This means measures should be implemented carefully, objectively, and proportionately, respecting the rights of all parties and minimizing the erroneous removal of lawful content. The technology used for automated detection, for instance, should be designed to minimize error rates.

1. **Rules on refraining from algorithmic content monitoring**

Hungarian law, in alignment with the EU framework, does not contain general rules that require platforms to refrain from using algorithmic content monitoring or other measures that influence user experience.

The central legal provision in this area is Article 8 of the DSA, which prohibits Member States from imposing a general monitoring obligation on platforms. This acts as a crucial safeguard, meaning that while a platform may choose to use algorithms for moderation, the state cannot mandate a system of universal, *a priori* surveillance. This protects against state-compelled censorship and respects users' fundamental rights to privacy and freedom of expression.

The NMHH published a related study in January 2025 and this concluded that the content and account moderation rules of very large online platforms are opaque, and that it would therefore be beneficial if, in the future, users could receive meaningful explanations from platforms if they are subject to restrictions. The study also highlights that such platforms, which are now unavoidable in the digitalized world, should provide much broader access to human administrators than they currently do, and to do so, they would need to employ significantly more staff.[[23]](#footnote-23)

The regulatory framework addresses the “black box” nature of algorithms primarily through transparency requirements. The DSA sets out that providers of intermediary services must include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information must include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It must be set out in clear, plain, intelligible, user-friendly and unambiguous language, and must be publicly available in an easily accessible and machine-readable format.[[24]](#footnote-24)

Regarding other measures influencing user experience, the DSA does not require platforms to refrain from algorithmic solutions either. Rather, it demands a high degree of transparency. For instance, platforms must inform consumers when a business applies personalized pricing based on automated decision-making and controllers operating such an automated decision-making mechanism based on AI cannot completely hide how their algorithm works, as they must inform the data subject of the logic used and its relevance and consequences for them before the processing starts. In this case, if the customer decides to consent to the processing of their personal data, in possession of the above information, they should also be given the possibility to opt-out from the personalized pricing scheme.[[25]](#footnote-25)

Furthermore, to mitigate significant risks, such as biased or discriminatory content targeting, or addictive behaviour that can be detrimental to maximizing their screentime, very large online platforms should analyse and assess annually the systematic risks arising from their algorithmic systems and implement reasonable, proportionate, and effective mitigation measures.[[26]](#footnote-26)

1. **Differences in liability privileges**

While the foundational liability exemptions in Articles 4-6 of the DSA are horizontal and apply equally to all forms of illegal content, the practical application of these privileges differs significantly across IP infringements, unfair competition cases, and other violations. These differences arise from specific national laws, distinct enforcement regimes, and the nature of the underlying rights being protected.

While the applicable legal frameworks—primarily the DSA, the E-Commerce Act, and relevant sectoral laws – share common safe harbour provisions derived from Articles 4 to 6 of the DSA (formerly Articles 12 to 14 of the E-Commerce Directive), their application varies substantially depending on the type of content, the identity of the complainant, and the nature of enforcement mechanisms. In the IP context, the liability regime is predominantly fault-based, supplemented by sector-specific rules, such as the stricter obligations imposed on Online Content-Sharing Service Providers (OCSSPs) under the Hungarian Copyright Act. A formal notice-and-takedown (NTD) procedure set out in the E-Commerce Act can offer a safe harbour if intermediaries follow it precisely. However, enforcement is largely driven by rightsholders through civil litigation, and one of the most pressing difficulties is the identification of anonymous infringers—complicated by data protection constraints, as illustrated by the Kúria’s decision in BH 2017.1.20. Remedies typically include injunctions, damages, and restitution of economic gains.

By contrast, in cases of unfair commercial practices and consumer protection, the legal framework encompasses the DSA, the Competition Act, the UCP Act, and the Advertising Act. Here, liability primarily rests with the business entity or advertiser responsible for the infringing content. Intermediaries, particularly neutral platforms, enjoy broader exemptions from liability, which are supported both by the general safe harbours of the DSA and specific exclusions under the Advertising Act. Notably, public enforcement predominates in this domain, with the HCA playing a central role. The HCA tends not to pursue platforms for user-generated content violations directly, but instead focuses on compelling platform operators to cooperate with investigations, such as by disclosing information or removing specific infringing content. Thus, the intermediary’s responsibility is framed more in terms of procedural cooperation with administrative authorities rather than fault or omission in content moderation.

For other forms of illegal content – especially defamation and hate speech – the liability framework invokes general tort law under the Civil Code and, in some cases, criminal liability under the Criminal Code. While content creators bear primary responsibility, intermediaries may become secondarily liable if they acquire actual knowledge of unlawful content and fail to act expeditiously. This principle, codified in Article 6 of the DSA and Hungarian transposition norms, is further nuanced by jurisprudence such as the ECtHR’s Delfi v. Estonia ruling, which allows for a stricter standard where the content is clearly unlawful and particularly severe. In this area, enforcement mechanisms may include both private civil claims and public criminal prosecution. Courts must continuously balance intermediary obligations against fundamental rights, particularly freedom of expression as protected by the Charter of Fundamental Rights of the EU and the European Convention on Human Rights.

Summarizing the above, the “difference” in liability privileges is less about the text of the exemption provisions themselves and more about the surrounding enforcement ecosystem. The platform's practical obligations are shaped by who is lodging the complaint (a private rightsholder, a state authority, or an individual citizen) and the remedy being sought (a simple takedown, a fine for non-cooperation, or damages for harm caused). This creates a spectrum of responsibility: for IP, the duty is one of procedural diligence; for unfair competition, it is one of cooperative compliance with authorities; and for other torts like defamation, it is one of reactive caution upon receiving clear notice.

**Mechanisms in Cases of Infringement**

Mechanisms to report content are established by (i) the DSA, relative to illegal content in general; and (ii) the E-Commerce Act in relation to the enforcement of certain intellectual property rights by right-holders.

1. ***Mechanisms to report IP violations***

Online platforms must provide mechanisms for reporting content that may violate intellectual property rights. Hungary's legal framework establishes two parallel systems for this purpose: a general “notice and action” mechanism under the DSA and a specific “notice-and-takedown” procedure for certain IP rights under the E-Commerce Act.

* 1. ***Detection of possible IP infringements***

Under both systems, the detection of possible infringements is primarily initiated by external parties, not the platform itself.

***DSA Notice and Action (NA):***To submit a report in the context of an NA mechanism (“**NA Report**”), reporters must provide the following information:

1. a sufficiently substantiated explanation of the reasons why the reporter alleges the information in question to be illegal content;
2. a clear indication of the exact electronic location of that information (e.g., relevant URLs) and, where necessary, additional information that enables the identification of the illegal content;
3. the name and email address of the reporter (with certain exceptions); and
4. a statement confirming the bona fide belief of the reporter that the information and allegations contained in the NA Report are accurate and complete.

***E-Commerce Act Notice-and-Takedown (NTD):*** This more formal procedure is specifically for holders of copyright, neighbouring rights, or trademark rights. The rightsholder must submit a notice in a private document with full probative force, detailing the subject matter of the infringement and the facts supporting the claim.

* 1. **Further processing procedure**

***DSA NA Procedure:***When an NA Report is made, the platform service provider must confirm receipt of the NA Report to the reporter, provided that the report includes the reporter’s electronic contact information.Thereafter, the service provider must decide on whether the reported content is indeed illegal. The DSA establishes the rules for such decision-making in a relatively vague manner: it stipulates only that the service provider must make its decision “*in a timely, diligent, non-arbitrary and objective manner*”. Relatedly, Act CIV of 2023 on Certain Rules regarding Internet Intermediary Services stipulates only that if a platform service provider becomes aware of illegal content, it must remove or disable access to such content “*without undue delay*”.After the service provider has made its decision, it takes measures based on such decision. Furthermore, it must notify the individual or entity who has published the content (“**Publisher**”) concerned with the NA Report about the service provider’s decision and the possibilities for redress of the decision (regarding redress, see below for more details). If the processing of the NA Report and/or the service provider’s decision-making involved automated means, the aforementioned notification must also include information thereof.

**E-Commerce Act NTD Procedure**: This procedure is more prescriptive. The right-holder must submit the NTD Notice in a private document with full probative force or in an authentic instrument. The NTD Notice must include the following details:

1. the subject matter of the infringement and the facts supporting the infringement;
2. the particulars necessary for the identification of illegal information;
3. the right-holder’s name, residence address or registered office, phone number and electronic mail address.

If the right-holder is represented, the representative’s authorization, recorded in a private document with full probative force or in an authentic instrument, must also be attached to the NTD Notice. Within twelve hours of receiving the NTD Notice, the platform service provider is required to remove or disable access to the content specified in the NTD Notice. Additionally, the service provider must indicate who made the NTD Notice and the alleged infringement that caused the removal of content. Within three working days of receiving the NTD Notice, the service provider must also notify the Publisher, in writing, about the removal of content.

If the service provider receives an NTD Notice in relation to a content relative to which it has already acted upon based on a previous NTD Notice from the same right-holder, or its representative, then the service provider must refuse to remove or disable access to the content, unless such measures have been ordered by the court or an authority.

If the Publisher acknowledges the infringement or fails to lodge an objection within the mandatory time limit, or lodges an objection but fails to contain the mandatory particulars, the service provider must keep access to the illegal information disabled or keep it removed.

However, the Publisher may object to the service provider’s measures within eight days of the receipt of the service provider’s relevant notification. The objection must be recorded in a private document with full probative force or in an authentic instrument. The objection must include the following details:

1. the particulars for the identification of the content removed or to which access has been disabled, including the network address where it was previously hosted, and the particulars for the identification of the recipient of the service affected, as provided for in the E-Commerce Act for all content providers;
2. a statement, including justification, declaring that the information provided by the recipient of the service did not infringe upon the rights of the right-holder indicated in the NTD Notice.

After receiving the Publisher’s aforementioned objection, the platform service provider must make the content accessible again without undue delay and inform the right-holder thereof, unless the service provider removed or disabled access to the content was ordered by the court or an authority.

Thereafter, if in ten working days, the right-holder moves to enforce their claim relating to the infringement they alleged in the notification by

* initiating a civil law litigation, together with requesting the court to order the termination of the infringement; or
* initiating an order for payment procedure; or
* filing criminal charges,

and the court orders the temporary removal or inaccessibility of the content, then the service provider must comply with the court’s order within twelve hours after it receives the order. In such case, the service provider must indicate in the platform, again, who alleged the infringement and what is the allegation that caused the removal of content. Furthermore, within one working day after the service provider receives the court order, the service provider must notify the content publisher about the measures taken and send a copy of the court order.

* 1. **Timeframe**

As noted above, the timeframes are a key differentiator under the DSA and the E-Commerce Act NTD regimes:

* **DSA NA:** The DSA requires decisions to be made in a “timely” manner and action to be taken “without undue delay,” but does not set specific deadlines.
* **E-Commerce Act NTD:** This procedure imposes strict deadlines: 12 hours for the initial takedown upon notice, three working days to notify the publisher, eight days for the publisher to object, and ten working days for the rightsholder to initiate legal action after a counter-notice.
  1. **Consequences in case of failure to adhere to requirements**

Failure to comply with these requirements has significant consequences for platforms. The primary consequence is the loss of the liability exemption.

**DSA NA:** If the service provider does not comply with the above-detailed rules, the President of the NMHH may

* prohibit the service provider’s illegal conduct;
* impose obligations on the service provider to enforce the DSA and relevant Hungarian implementing laws;
* order the service provider to publish a notice or the decision on the home page of website in the manner and for the period specified in the decision and/or
* impose an administrative fine on the service provider, up to 6% of the service provider’s annual worldwide turnover in the preceding financial year.

Platform service providers who become aware of illegal content but do not take the measures necessary under applicable law are no longer exempt from liability in relation to the illegal content; therefore, right-holders might also claim compensation from such service providers [e.g., due to unlawful use of intellectual property, or damages sourcing from the infringement of Article 14 (4) of the DSA]. In extreme cases, non-compliance might also have criminal or misdemeanour law implications (e.g., due to the infringement of copyright). In case of NA Reports, it may be sufficient to have the content removed if the reporter demonstrates to the platform service provider that the reported content is likely illegal. This may provide protection to the right-holders but, in some cases, might give rise to unjustified content removals.

**E-Commerce Act NTD:** Platform service providers who become aware of illegal content but do not take the measures necessary under applicable law are no longer exempt from liability in relation to the illegal content; therefore, right-holders might also claim compensation from such service providers (e.g., due to unlawful use of intellectual property and damages).

In extreme cases, non-compliance might also have criminal or misdemeanour law implications (e.g., due to the infringement of copyright). If the relevant non-compliance issue also infringes the DSA, relevant legal consequences may also apply (see more details in Section 3.1.2. above).

In case of NTD Notices, the NTD Notice itself may result in the removal of content. However, the fact that the Publisher’s objection may lead to the republishing of illegal content might affect the efficiency of NTD mechanisms negatively. Furthermore, considering that Hungarian laws must be interpreted in accordance with EU laws, certain rules on NTD Notices in the light of the DSA (e.g., regarding the Publisher’s objection) might lead to interpretational issues.

Compliance in good faith with the NTD procedure immunizes the intermediary from all forms of liability for the IP infringement in question. In practice, this means that if a platform diligently follows the notice-and-takedown steps for, say, for a copyright infringing image or a trademark-infringing product listing, it will not be liable for that infringement – neither for damages nor fines – and can only be subject to, at most, an injunction to remove the content (which it has already done by following the procedure).

This Hungarian NTD system is relatively robust and provided a clear legal pathway for IP owners to get infringing content removed quickly. One drawback, however, was that once content was taken down, rightsholders often struggled to identify the infringer for further legal action; intermediaries in Hungary frequently refused to disclose user data without a court order, citing data protection laws. This has been a long-standing enforcement challenge: even though Hungarian law (and EU law via the IPR Enforcement Directive) in theory allows courts to compel intermediaries to give up information on infringers, privacy concerns and the lack of explicit pre-litigation disclosure rules made it difficult for rights holders to obtain the identities of anonymous online wrongdoers in the absence of criminal proceedings. In the case published under reference number BH 2017.1.20, the Hungarian Kúria addressed the interpretation of Section 94(1)(d) of the Copyright Act, which prescribes data disclosure obligations. The central issue of the case was whether an internet service provider (ISP) being an online intermediary could be compelled to disclose personal data in the context of a copyright infringement proceeding without the consent of the data subjects concerned. The Kúria held that an ISP, acting as a mere conduit intermediary service provider, cannot be compelled to disclose the names and addresses of individuals associated with IP addresses in civil proceedings initiated for copyright infringement. Data disclosure by the ISP is only permissible where expressly provided by law—for instance, for national security or criminal law enforcement purposes—but not in civil proceedings, unless the data subject has given consent. This interpretation aligns with Section 13/A(6) of the E-Commerce Act which stipulates that user data processed in the context of using the service may not be linked to the user’s identifying data and may not be disclosed to third parties without the user’s consent. The judgment underlines the fundamental legal principle of the primacy of personal data protection. Data disclosure constitutes personal data processing, which is subject to strict conditions under data protection laws. According to the ruling, profiling inferences drawn from internet usage and user habits based on an IP address may be linked to a specific individual and relate to the most intimate aspects of one’s personality. In certain cases, such data may even qualify as special categories of personal data, to which more stringent rules apply under personal data protection regulations and such data may not be disclosed without legal authorization.

1. **Other remedies against platforms**

Beyond the reporting mechanisms, other legal remedies and requirements can be directed against platforms in cases of IP or unfair competition infringement. Even when an intermediary is exempt from liability for damages, Section 7(5) of the Hungarian E-Commerce Act clarifies that an intermediary's exemption from liability under DSA Articles 4–6 does not prevent an injured party from seeking court-ordered injunctions against the intermediary (alongside the primary infringer) to prevent or stop the ongoing infringement. In this context, Courts can and do issue such injunctions without needing to establish that the intermediary itself was at fault – for instance, a court may order a website host to remove specific infringing content or to prevent further access to it, even though the host is protected from damages liability. By contrast, if an intermediary fails to remove content despite having actual knowledge of its illegality (for example, ignoring a valid takedown notice), it can then face the full spectrum of civil liability, including damages for ongoing infringement or contributory liability. In line with European jurisprudence, Hungarian courts cannot impose a blanket obligation on intermediaries to filter or police all user content, since that would conflict with the no-monitoring rule and fundamental rights They can, however, impose targeted measures: Hungarian law (echoing CJEU guidance) allows injunctions that might require an intermediary to prevent a specific infringement from recurring, as long as such measures are proportionate and do not amount to general surveillance. For example, if a particular seller on a marketplace repeatedly sells counterfeit goods, a court injunction could require the platform to suspend that seller and even to proactively bar re-listing of the same counterfeit items – but the platform cannot be ordered to scrutinize all user listings in general.

If a platform loses its liability exemption by failing to act on actual knowledge of illegality, it faces the full range of civil remedies available under Hungarian law. These include:

* A court declaration establishing the fact of the infringement.
* A cease and desist order (injunction).
* Financial remedies, including compensation for damages under the Civil Code and restitution of economic gains achieved through the infringement. Court practice indicates that the minimum amount of economic gain is often calculated as the value of an unpaid royalty or license fee.

In IP cases, preliminary injunctions are a particularly important remedy and can be requested even before a full lawsuit is filed. Recent CJEU case law (Bayer v Richter/Exeltis) has clarified that a plaintiff is not automatically liable for damages from a wrongful injunction if they did not act abusively, which may encourage their use by rightsholders.[[27]](#footnote-27)

In the context of unfair competition, the HCA has the power to order platforms to provide information during investigations and can compel them to execute a takedown order if the primary violator fails to comply. Non-cooperation with an HCA order can result in significant fines.

1. **Use of “trusted flaggers”**

Hungary has formally established the use of “trusted flaggers” in accordance with Article 22 of the DSA.

* 1. **What criteria are applied?**

In case of trusted flaggers under Article 22 of the DSA, the standard trusted flagger criteria apply, established by Article 22 (2) DSA, meaning that an entity may be designated as a trusted flagger if it (a) has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content; (b) is independent from any provider of online platforms; and (c) carries out its activities for the purposes of submitting notices diligently, accurately and objectively.[[28]](#footnote-28) Apart from the standard DSA-based criteria, Hungarian law establishes further criteria that applicants for trusted flagger status must possess minimum of five years' experience in media monitoring or analysis, or in online content monitoring or analysis, specifically in relation to the detection, identification, and reporting of illegal content, as well as the systemic risks defined under Article 34 DSA.[[29]](#footnote-29) The President of NMHH keeps an official, public registry of trusted flaggers. Only organizations established in Hungary that meet both DSA and NMHH decree requirements may be designated. The designation is made by an official administrative decision, which also covers potential suspensions or revocations. The registry includes: name, seat, and email address of the trusted flagger, their designated area(s) of expertise, suspension or revocation information (if applicable). Trusted flaggers must notify the President of any changes in their eligibility or data within 15 days.

* 1. **How are these entities identified, nominated, and/or appointed?**

Entities are designated as trusted flaggers by the President of the NMHH through an official administrative decision. The NMHH maintains a public registry of all designated trusted flaggers. Currently, only organizations established in Hungary that meet both the DSA and the specific Hungarian requirements can be designated.

Based on Sections 149/B-149/D of Act C of 2003 on Electronic Communications, the NMHH operates an **online information and assistance service** in the interest of promoting the safe use of the internet, in pursuing an objective in the public interest, such as the protection of minors, raising awareness, help to mitigate online content depicting violence, hate and other forms of potential abuses, acting within a capacity other than a public authority, within the framework of tasks carried out in the public interest. This online information and assistance service is called **Internet Hotline** and it is operating since 2011.[[30]](#footnote-30)The Internet Hotline is not entitled to investigate content appearing in media service or press products; unsolicited electronic advertising (spam); legal disputes concerning copyright matters; consumer complaints about online shops; privacy notices, or lack thereof; cases of misuse of the Internet that fall under the exclusive competence of another authority, court or other public body. From 25 October 2024, Internet Hotline also acts as a **trusted flagger** under the DSA. Internet Hotline can submit notices as a trusted flagger relating to content published without consent; child pornography; online harassment; racist content; content inciting hatred against a community; content promoting or encouraging the use of illegal psychoactive substances; content inciting or promoting violent or illegal acts; phishing content; and other content harmful to minors.

Therefore, in Hungary, the DSA’s trusted flagger framework and the national reporting framework work in parallel with each other, with the Internet Hotline being the first (and currently only) DSA trusted flagger in Hungary.

* 1. **Prioritized treatment of notices**

Under the DSA trusted flagger framework, notices submitted by the Internet Hotline and other future trusted flaggers shall be given priority and be processed and decided upon without undue delay under Article 22 (1) of the DSA.

Under the Hungarian reporting framework, when an internet abuse is detected, it may be reported through the reporting platform of Internet Hotline. Upon receipt of such a report, the NMHH shall act with a view to safeguarding the public interest, in the form of legal aid, where the circumstances indicate the probability of internet abuse on the basis of the Internet Hotline rules of procedure[[31]](#footnote-31). An inquiry upon receipt of a report is not an administrative proceeding, the NMHH may not exercise any regulatory competence and may not take regulatory action, the report shall not make a regulatory case. The NMHH examines the report and if it is manifestly unfounded, or if the case reported is not covered by the internet hotline regulations, it closes the case without making further inquiries. If based on the inquiry NMHH establishes the probability of internet abuse, it shall contact the content and hosting provider of the online content involved by transferring the information available for the purpose of investigating the online content, and to take appropriate measures consistent with the outcome of the inquiry. The service provider contacted shall inform NMHH of the measures implemented. If the report raises the probability of a crime that is punishable not on private motion, the NMHH shall forward the report within one working day of receipt to the competent investigating authority.

Therefore, there is no express legal requirement to prioritize reports by the Internet Hotline, but the involvement of the NMHH and the structure of the Internet Hotline system create a **de facto prioritization** in handling such reports, especially in child protection and criminal content contexts.

1. **Requirements before content removal and impact on efficiency**

Generally, a court order is not a prerequisite for the removal of content that potentially infringes intellectual property rights in Hungary. The primary mechanisms – the DSA's NA system and the E-Commerce Act's NTD procedure - are designed as extra-judicial processes. They are triggered by a notice from a rightsholder or another party, which then places an obligation on the platform to assess the content and act without needing prior judicial authorization.

A court order becomes the ultimate authority in disputed situations. For example, under the Hungarian NTD procedure, if a content publisher submits a valid counter-notice to a takedown, the platform is obligated to restore the content. At that point, the rightsholder's only recourse to have the content removed again is to initiate formal legal proceedings and secure a court order compelling the takedown.

The efficiency of these notice procedures is significantly affected by this structure. The Hungarian NTD procedure is a double-edged sword. On one hand, it is highly efficient for achieving an initial takedown, as the strict 12-hour deadline provides a rapid, powerful tool for rightsholders to remove infringing content quickly.

On the other hand, its efficiency is severely undermined by the counter-notice provision. An infringer can easily restore the content by lodging an objection, shifting the burden and cost of initiating a full lawsuit back onto the rightsholder. This problem is compounded by a major practical and legal obstacle: the difficulty of identifying anonymous infringers. The Kúria's landmark ruling in case BH 2017.1.20 established that data protection principles prevent courts from compelling service providers to disclose user data in civil IP proceedings. This creates an “enforcement black hole”: a rightsholder can successfully get content taken down but is then unable to identify the infringer to sue them, preventing any definitive resolution or claim for damages. This renders the NTD system effective at treating the symptom (a single instance of infringement) but often inefficient at curing the underlying disease (the infringer's ongoing activity). The general slowness of the Hungarian judicial system further amplifies this inefficiency, as any ensuing litigation can take years to resolve.

1. **Appeals against content removal decisions**

There are measures in place to appeal content removal decisions based on IP infringements. The DSA establishes a multi-tiered system of redress for users whose content has been removed. Those concerned with the platform service provider’s decision made in the context of NA mechanisms under the DSA (see more details in Section 6 above) have the following options for redress:

1. **Internal complaint handling system:** they can use the platform service provider’s internal complaint handling system to lodge complaints against the aforementioned decision, by electronic means and free-of-charge – recipients of the platform service provider’s services must have access to such system at least for six months following the service provider’s aforementioned decision;
2. **Out-of-court dispute resolution:** they can select any out-of-court dispute settlement body, certified in accordance with the DSA, to resolve any dispute in relation to the aforementioned decision;
3. **Judicial redress:** they can file a civil lawsuit to challenge the platform service provider’s decision.

**Fundamental Rights**

1. **Safeguards balancing IPR and fundamental rights**

Hungary has instituted legal safeguards to maintain balance between the enforcement of intellectual property rights (“**IPR**”) and the protection of fundamental rights. Meanwhile a more thorough response demands a concise review of the Hungarian constitutional context of the raised issue, as it pertains particularly to legal relationship with fundamental rights.

**11.1 Constitutional safeguards**

The Fundamental Law of Hungary comprehensively regulates individual and collective fundamental rights and obligations throughout the entire Hungarian legal system as well as the legal hierarchy[[32]](#footnote-32) as the foundation stone of the Hungarian legal system.[[33]](#footnote-33) Therefore, Article T)(3) of the Fundamental Law of Hungary[[34]](#footnote-34) makes it unavoidable to identify the fundamental legal roots of the protection of IPR.

As the foundation of the legal system of Hungary, the Fundamental Law of Hungary is governing all areas of law, including IPR, albeit in an indirect way. The preamble of the Fundamental Law of Hungary, the National Creed asserts that “*We* [the people of Hungary] *are proud of the outstanding intellectual achievements of the Hungarian people*”, while the further textual examination of the Fundamental Law reveals an absence of any mention of intellectual property. Despite the absence of explicit provisions in the Fundamental Law pertaining to the protection of IPR, the legal framework for safeguarding intellectual property is predicated on constitutional principles and can be extrapolated from certain fundamental rights. The Constitutional Court of Hungary (“**Constitutional Court**”) has previously established a link between the right to property and intellectual property.

Pursuant to Article XIII(1) of the Fundamental Law of Hungary, “*Everyone shall have the right to property* […]*. The ownership of property shall entail social responsibility*”. The Constitutional Court consistently interprets the provision of the Fundamental Law of Hungary protecting the right to property in a broad manner. The subject of property protection in the constitutional sense is not only the ownership of things, but it also includes certain other property rights and claims. From this point of view, it is of decisive importance that the subject of this extended protection of right to property may also be a lasting right of property value (but not qualifying as ownership in the civil law sense). The Constitutional Court has established in its early case law, which is still authoritative today[[35]](#footnote-35), that the constitutional protection of right to property clause “*applies not only to the right of ownership, but also to all property rights related to it* [...] *and also ensures the protection of other property rights within the scope of property protection*.”[[36]](#footnote-36) Based on this theoretical approach, the interpretation of the Constitutional Court also included industrial property rights within the scope of constitutional property protection[[37]](#footnote-37). Acting on the basis of the Fundamental Law, the Constitutional Court also proceeds from the general approach that, in the context of industrial property rights, property rights are considered to be legal objects protected by the right to property. At the same time, the Constitutional Court also pointed out that the protective function and role extend only and exclusively to the protection of already acquired property rights, but not to pending, unassessed applications, requests or claims. If the application for industrial property protection (in this case, trademark registration) remained in the request stage, the right to the property in question could not have been infringed because it had not yet been acquired.[[38]](#footnote-38) The infringement of certain partial rights of ownership may lead to a violation of fundamental rights: “[…] *the Fundamental Law of Hungary protects specific rights existing at a specific point in time, recognized by law as fundamental rights to property: based on the fundamental right to property, the legislature is generally obliged to respect those rights which constitute components of the fundamental right to property in the constitutional sense.*”[[39]](#footnote-39) Therefore, as an interim conclusion, given that IPR is derived from the right to property as guaranteed in the Fundamental Law of Hungary, consequently, any collision requiring legal safeguard to ensure balance between IPR and fundamental rights shall also be examined within fundamental legal context.

In light of the aforementioned considerations, circumstances requiring to maintain balance between the enforcement of intellectual property rights and fundamental rights may primarily emerge from conflicts between different fundamental rights and the right to property and its specific partial rights. In the event of a conflict between different fundamental rights, constitutional rules for resolving such conflicts, primarily the standard of restriction of fundamental rights and general and specific tests ensure balance between fundamental rights.

Pursuant to Article I(3) of the Fundamental Law of Hungary establishes the general standard stating that certain fundamental rights may only be restricted by law, and that “*fundamental right*[s] *may only be restricted in order to enforce another fundamental right or to protect a constitutional value, to the extent that is absolutely necessary and proportionate to the objective pursued, and with respect to the essential content of the relevant fundamental right.*” This provision defines the fundamental legal standard for restricting fundamental rights, also known as the “necessity and proportionality test”. Based on the necessity and proportionality test, three main questions need to be examined if a conflict between different fundamental rights can only be resolved by restricting fundamental rights: (i) whether the restriction has a legitimate, i.e. constitutional, legislative purpose, (ii) whether the restriction is necessary to achieve the desired objective, and (iii) whether the restriction is proportionate to the desired objective. The necessity and proportionality test may also be supplemented by the requirement of the least restrictive solution, which means that the legislator shall find a regulatory solution that restricts the fundamental rights in question as little as possible overall. The essence of the test is that all elements must be satisfied for the restriction to be constitutional.

In addition to the necessity and proportionality test, as implied in Article XIII(1) of the Fundamental Law of Hungary[[40]](#footnote-40) the so called “public interest test” shall be applicable in cases of conflict between the right to property and public interest. Therefore, the right to property may be restricted in the public interest in a manner proportionate to that interest, also in connection with the social responsibility associated with property. In this regard, the Constitutional Court reiterated its oft-repeated position as follows: “*Pursuant to Article XIII(1) of the Fundamental Law, everyone has the right to property, and property also entails social responsibility.* […]. *However, the restriction of any element of the right to property only constitutes a restriction of the right to property as a fundamental right and is therefore only unconstitutional if it is not unavoidable, if there are no compelling reasons for it, and if the severity of the restriction is disproportionate to the aim pursued by the restriction.*”[[41]](#footnote-41)

In addition to the necessity and proportionality test, other special tests may be applied, which represent even more sophisticated methods of examination with regard to individual fundamental rights. For example, the Constitutional Court adopted[[42]](#footnote-42) the “*clear and present danger*” or “*actual malice*” test developed by the Supreme Court of the United States[[43]](#footnote-43) in relation to freedom of expression. According to this test, not only the result of the communication but also, in certain cases, the speaker’s intention must be taken into account.

Other than the Fundamental Law of Hungary, legal standards originating from international obligations, as part of the Hungarian legal system[[44]](#footnote-44), are also provides a legal framework for a modus vivendi in terms of IPR and fundamental rights such as European and global international agreements that treats IPR as fundamental rights such as European Convention on Human Rights (“**ECHR**”)[[45]](#footnote-45), primary and secondary law of the European Union (“**EU**”) such as the Treaty on the Functioning of the European Union (“**TFEU**”) and the Charter of Fundamental Rights (“**CFR**”)[[46]](#footnote-46), the Agreement on Trade-Related Aspects of Intellectual Property Rights (“**TRIPs**”)[[47]](#footnote-47).

**11.2 Specific safeguards in IP related legislation**

In accordance with the provision contained in Article I(3) of the Fundamental Law of Hungary, pursuant to which fundamental rights may only be restricted by law, the second level of legal safeguards are contained in certain IP specific legislation or IP specific provisions of other legislation.

First, given that the law of intellectual property is a legal field within civil law[[48]](#footnote-48), it is necessary to mention the legal safeguards contained in the Civil Code[[49]](#footnote-49) as a background norm for separate IP legislation. Legal principles of the Civil Code provides general safeguarding measures, such as (i) the principle of good faith and fair dealing[[50]](#footnote-50), which help to draw the boundaries of private autonomy and the free exercise of rights, (ii) the principle of reasonable conduct[[51]](#footnote-51), which as a standardized set of requirements allows the court to make a flexible assessment tailored to the countless differences in life situations or (iii) the prohibition of abuse of rights[[52]](#footnote-52), which prohibits the exercise of rights contrary to the purpose of subjective rights.

IP related legislation, such as the Copyright Act, the Trademark Act, or the Patent Act, contain numerous exceptions and limitations aimed at protecting fundamental rights. These include, for example, compulsory license due to failure to commence exploitation or dependency of patents[[53]](#footnote-53), the principle of fair use[[54]](#footnote-54), the right of exhibition or in other words the freedom of panorama (i.e. the freedom to photograph works of art in public spaces)[[55]](#footnote-55), and free use for educational, research, or news reporting purposes,[[56]](#footnote-56) or the period of protection[[57]](#footnote-57) and the requirements for use of the trademark[[58]](#footnote-58), as well as the legal consequences of failure to comply with these requirements, in particular the possibility of using this circumstance as a defense in trademark infringement proceedings.[[59]](#footnote-59) These exceptions ensure that intellectual property rights do not hinder cultural access, education, research, or access to information of public interest.

Last but not least, as keystone or *ultima ratio* of the Hungarian sanctional regime, Act C of 2012 on the Criminal Code (“**Criminal Code**”) provides comprehensive criminal law protection for IPR, including industrial property rights, copyright and related rights, such as property and personal rights relating to intellectual creations. The provisions of the Criminal Code are framework provisions and are supported by numerous background legal provisions, not only in domestic law but also in international treaties promulgated by law and in European Union legal acts.

**11.3 Procedural safeguards**

On the procedural level, Act CXXX of 2016 on the Code of Civil Procedure (“**CCP**”) contains mechanisms aimed at enforcing intellectual property rights and maintaining a balance between fundamental rights. These tools ensure that IP rights are not enforced in a way that disproportionately restricts the rights of others, and they pay special attention not to violate freedom of expression, the right to information, or other fundamental rights.

One such tool is the application of provisional measures (or interim injunctions). On this basis, courts may order interim measures in IP cases, such as the temporary removal of infringing content or the cessation of the infringement. At the same time, the court must assess the proportionality of the measure and whether there is a risk of irreparable harm in terms of the party concerned. Such measures may only be ordered if this risk justifies the temporary restriction of another person’s rights.[[60]](#footnote-60)

Furthermore, Hungary has integrated EU directives such as the Directive 2004/48/EC on the enforcement of intellectual property rights (hereinafter: “**IPR Enforcement Directive**”), which obliges member states to ensure that IP enforcement is fair, equitable, and proportionate. Hungarian law provides multiple legal avenues for IP enforcement while incorporating judicial oversight to prevent disproportionate outcomes. For example, interim injunctions are only granted if the harm to the rights holder clearly outweighs the restriction on the defendant’s rights, reflecting a proportionality test that protects both parties’ fundamental rights.

Overall, the Hungarian legal system seeks, at several levels and through various means, to ensure that the protection of IP rights does not come at the expense of other fundamental rights and that the enforcement of such rights is always in line with the principles of proportionality and fairness.

**11.4 Competition law**

Despite its seemingly divergent subject matter, competition law can also be regarded as a safeguard that serves to maintain the balance between intellectual property rights and fundamental rights. Article M)(1)-(2) of the Fundamental Law of Hungary as a constitutional doctrine provides that “*(1) The economy of Hungary shall be based upon work as the very foundation of productivity, and upon the freedom of enterprise. (2) Hungary shall ensure the conditions of fair economic competition, act against the abuse of a dominant economic position and protect the rights of consumers.*” While Article M) – as the constitutional basis of Hungarian competition law – is not an independent constitutional right guaranteed by the Fundamental Law of Hungary[[61]](#footnote-61), both economic competition and protection of consumer rights are state obligations linked to specific fundamental rights, for example the freedom of enterprise[[62]](#footnote-62) and the right to property[[63]](#footnote-63). Therefore, a role to balance between fundamental rights and IPR can be attributed to the obligation of the Hungarian State to establish and maintain the institutional system that protects and ensure fair competition and consumer rights.[[64]](#footnote-64) The aforementioned obligation to ensure fair competition requires the establishment of institutions to protect the freedom of enterprise and other fundamental rights necessary for the maintenance of fair competition, including right to property and freedom of movement. Fair competition is achieved through the enforcement and protection of individual fundamental rights.[[65]](#footnote-65)

Among the objectives of competition law, it is perhaps the promotion of innovation that is most closely linked to the objectives of intellectual property rights. Both ensuring fair competition and providing an appropriate and productive environment for intellectual property rights protection can foster creativity, including innovation, although competition law focuses primarily on innovation by economic sense, while intellectual property rights focus on the creative activity of natural persons and the encouragement thereof.

It should be noted that the so-called block exemption regulations governing specialization[[66]](#footnote-66), R&D[[67]](#footnote-67) and vertical agreements[[68]](#footnote-68) relating to the prohibition of agreements restricting competition laid down in Article 101 TFEU and Section 11 of the Hungarian Competition Act[[69]](#footnote-69) also contain provisions on intellectual property rights. The prohibition of abuse of dominant position laid down in Article 102 TFEU and Section 21 of the Hungarian Competition Act includes also abusive patent strategies as an IP specific exclusionary abuse thus limiting patent rights to a certain extent based on the public interest.

Therefore, the provisions of Hungarian competition law[[70]](#footnote-70) but also consumer protection law[[71]](#footnote-71) may also be relevant from an intellectual property perspective. In addition to the national counterparts of rules on the prohibitions and provisions already mentioned in terms of EU law, domestic competition law, more precisely the prohibition of unfair competition regulates behaviours such as passing off[[72]](#footnote-72) and the prohibition of comparative advertising[[73]](#footnote-73), which have close links to trademark law, therefore effect on the enforcement of IPR.

In summary, Hungary has implemented a legal framework that safeguards fundamental rights while enforcing IP laws. This framework includes constitutional provisions, statutory limitations within the Copyright Act, adherence to EU directives, and robust judicial oversight. Together, these elements ensure a balanced approach to IP enforcement that respects fundamental rights.

1. **Cases challenging IPR enforcement**
   1. **Freedom of expression**
2. **Social media case**

Recently, one of the most relevant judgement in terms of the raised issue was the decision of the Kúria no. Pfv.IV.20.914/2023/7., which examined the legal relationship between freedom of contract and freedom of expression in the context of social media platforms. Although the case serving basis for the judgment had primarily a contract law focus, it indirectly affected certain aspects of freedom of expression, the right to equal treatment, and freedom of contract as a private law branch of freedom of enterprise. Contract law, as a key component of the disposal of property rights in terms of IPR has particular relevance in connection with the raised issue as contracts are the legal vehicles by which IPR can be lawfully used by third parties and are essential tools by which IP owners can monetize their rights.

According to the facts of the case, a politically exposed person filed a lawsuit against an international social media platform provider for deleting the social media pages of the plaintiff, partly due to content considered to be hate speech. Among other things, these posts stigmatized people of roma origin, immigrants and ethnic minorities as violent or criminal. The plaintiff requested the court of first instance to declare that the defendant, by blocking the social media pages in question, had infringed the right to freedom of expression and its right to contact of the plaintiff. In contrast, the defendant contended that its services were governed by a private law contract, which incorporated the terms and conditions it had established, including the community guidelines and other rules governing access, which the users, including the plaintiff, had accepted upon registration. The aforementioned stipulations delineate the categories of behaviour that are deemed to be in contravention of the stipulated community guidelines. This enables the defendant, in its capacity as the service provider, to prohibit users’ access. The actions of the plaintiff were in direct contravention of the stipulated general terms and conditions, thereby establishing a legitimate basis for the termination of the service in accordance with the established legal framework.

The court of first instance dismissed the claim of the plaintiff, stating that the defendant did not breach the contract by blocking the pages of the plaintiff and, in the absence of such a breach, did not infringe the personal rights of the plaintiff.[[74]](#footnote-74) The court of second instance partially amended the decision and found that the defendant had violated the right of the plaintiff to maintain contact by deleting one of its social media pages, where the plaintiff did not posted content which would be in contravention of the stipulated community guidelines.[[75]](#footnote-75) The plaintiff filed a request for extraordinary review against the decision concerning the deletion of its other social media page. The Kúria upheld the final judgment.

In its judgment, the Kúria found that the lower courts had correctly proceeded on the basis that the assessment of this issue should not be based on the scope of interpretation defined by the Constitutional Court for the examination of freedom of expression as regulated in Article IX(1) of the Fundamental Law of Hungary. During the registration process it is necessary for the conclusion of the service contract to accept the general terms and conditions, without accepting such terms, the plaintiff would not have been able to use the defendant’s services. Therefore, the content of these terms and conditions had to be examined during the legal dispute. Consequently, in evaluating the purported violation of contract, the relevance of the plaintiff’s personal perceptions of offensiveness to third parties was deemed irrelevant. Instead, the focal point of the assessment was the content of the statement in question, which was to be examined and classified in accordance with the defendant’s delineation of hate speech. Furthermore, the Kúria underlined that courts are required to identify the fundamental rights aspects of a case within the scope of interpretation provided by the law. Furthermore, courts are required to interpret the legal provisions applied in their decision with regard to the constitutional content of the fundamental right concerned. However, this is subject to the condition that the party specifically identifies the alleged violation of the law and the reasons for it in its request for review. A reference to a violation of a particular article of the Fundamental Law of Hungary does not, in itself, constitute grounds for reviewing the merits of a final judgment, as the provisions of the Fundamental Law of Hungary are enforced through specific substantive and procedural laws.[[76]](#footnote-76)

The plaintiff filed a constitutional complaint against the decision of the Kúria which is still pending before the Constitutional Court under case number IV/02708/2024. According to the complaint, rules restricting freedom of expression must be interpreted restrictively, and the Fundamental Law of Hungary protects opinions regardless of their value or truth content based on the well-established practice of the Constitutional Court. In contrast, the decision of the court of second instance upheld by the decision of the Kúria, violates the right of the plaintiff to freedom of expression by interpreting the general terms and conditions in an extensive manner and attributing an arbitrary meaning to the communication in question, while at the same time making a value judgment.

1. **“*Ne bántsd a magyart*” case**

Challenging the enforcement of intellectual property rights related to right to a fair trial recently became an issue in the so called “*Ne bántsd a magyart*”[[77]](#footnote-77) case. As to the factual background of the case, the Hungarian Intellectual Property Office (“**HIPO**”) rejected the trademark application for the colorful graphic symbol “NE BÁNTSD A MAGYART, MERT PÓRUL JÁRSZ!” (Do not thread on Hungarians, or you'll get hurt!) on the grounds of conflict with public morals.[[78]](#footnote-78)

A skull and cross axes with a hat

AI-generated content may be incorrect.(*Illustration: the subject of the trademark application in question. Source: HIPO trademark database, e-records*[[79]](#footnote-79))

In its decision, the HIPO found that the figurative sign contained an offensive and crude exhortation and threat, the figurative element of which consisted of a drawing of a human skull (death’s head) and crossed weapons symbolizing human shinbones. The textual part of the figurative element clearly conveys this threatening content to Hungarian speakers, while the figurative element is well known and understandable regardless of language skills. The skull may refer to death and transience, but it can also be a warning sign if something is deadly (e.g., poisonous substances). The HIPO found that when consumers see the verbal indication combined with the graphic, they are confronted with a harsh warning or threat that may cause disapproval among the **majority** of society, repulsion among adult consumers, and even fright or fear among children.

The decision of the HIPO was upheld by the Budapest Metropolitan Court.[[80]](#footnote-80) In the proceedings at the first instance, the applicant argued that the warning shown on the graphic symbol could not be contrary to public morality, since the Fundamental Law of Hungary guarantees freedom of expression and the right to defend oneself against unlawful attacks directed against or threatening a person or property. The applicant reiterated that during the administrative proceedings several references were made to several authors who had included the contested slogan in the titles of their books (first Miklós Zrínyi, later several other publicists: Mózes Gaál, Lajos Für, Ferenc Donászy, József Szájer). The inscription in question also appeared on the barrel of the only cannon found belonging to Áron Gábor.

The court agreed with the position of the HIPO regarding the conflict between public morality and the pictorial symbol. According to the court, the HIPO correctly concluded that the slogan in question, without the additional text “*... you'll get hurt!*”, did not constitute a threat, but rather expressed a desire to avert danger to Hungarians and to put an end to behaviour threatening Hungarians. However, with the addition of the phrase “*... you'll get hurt!*”, the meaning of the text as a whole changes; it no longer expresses a wish or desire, nor is it a warning, but a direct, unambiguous threat.

The applicant filed an appeal against the decision of the court of first instance. The court of second instance shared the view of the court of first instance that the combined sign was not eligible for trademark protection due to its offensive or disturbing nature, therefore upheld the decision of the court of first instance.[[81]](#footnote-81)

* 1. **Right to a fair trial**

Challenging the enforcement of intellectual property rights related to right to a fair trial recently became an issue in the so called “Szűztea”[[82]](#footnote-82) case. As the factual background to the “Szűztea” case, upon a request for cancellation, the HIPO ordered the cancellation of the word trademark “SZŰZTEA”. The applicant initiated legal proceedings against the decision of the HIPO in which the court of first instance amended the decision of the HIPO and rejected the opposing party’s request for cancellation of the trademark, and the court of second instance upheld the decision of the court of first instance.

Based on the opposing party’s request for review, the Kúria (Supreme Court of Hungary) set aside the final decision, amended the decision of the court of first instance and rejected the applicants’ request for amendment. In its reasoning, the Kúria stated that it was not disputed in the proceedings that the designation in question did not have distinctive character. When deciding on the application for cancellation of the trademark, it had to be assessed whether the evidence provided by the applicant was sufficient to establish that the designation had acquired distinctive character through use.

When assessing the evidence pursuant to Section 206(1) of the CCP, the lower courts, contrary to the position of the HIPO, concluded that the volume and manner of use justified the acquisition of distinctive character. The Kúria ruled that the courts had reached an incorrect conclusion affecting the merits of the case when assessing and comparing the data and evidence taken into consideration, and therefore considered it justified to re-examine the evidence, within the narrow limits applicable in review proceedings. In doing so, the Kúria, agreeing with the findings of the HIPO, concluded that the applicant’s use of the designation did not meet the criteria for use as a trademark because it could not be established that the designation was used consciously, consistently, and for the purpose of indicating origin as a product designation.[[83]](#footnote-83)

The applicant filed a constitutional complaint against the decision of the Kúria ordering the cancellation of the trademark registration which was rejected by the Constitutional Court.[[84]](#footnote-84) The petitioners sought to substantiate their petition by invoking the right to a fair trial, including the right to a public hearing. In their view, the Kúria, without holding a hearing, based its decision on new legal grounds that had not been raised either before the court of first instance or before the court of second instance.

The Constitutional Court pointed out that the principle of hearing, oral proceedings and directness are among the fundamental principles of civil proceedings. However, it does not constitute a violation of these fundamental principles, which have been elevated to the status of constitutional rules, if the law allows the court to decide on a motion outside of a hearing, particularly in extraordinary legal remedy proceedings, such as the review process of the Kúria. The mere fact that a hearing is not held does not, in itself, constitute a violation of a constitutional procedural right, provided that there is no other violation of procedural or substantive fundamental right.

After examining the nature of the underlying court proceedings, the Constitutional Court found that the right to a fair trial had not been violated for the following reasons. The right to a fair trial does not imply that a public hearing must be held or that the right to appear in person must be guaranteed in all proceedings and before all courts. In the case in question, the Kúria acted in a non-litigious proceeding, in which the legislation itself provides that the parties concerned could not request a hearing. The Kúria was in fact a fourth instance court, where the unconditional application of the hearing principle would constitute an infringement of other procedural principles (simplification and timeliness of the proceedings, as well as their completion within a reasonable time limit) and would thus impede the enforcement of the parties’ rights guaranteed by the Fundamental Law of Hungary.

Another case relevant case was about granting public health related compulsory licenses by the HIPO without the patentee being heard. After lower courts rejected the appeals of the patentee, it submitted a complaint to the Constitutional Court.

In October 2023, the Constitutional Court published its decision and annulled all the decisions of the HIPO and the lower courts due to the violation of the Fundamental Law of Hungary. According to the Constitutional Court the HIPO deprived the patentee of client status, which is a serious limitation of fundamental rights. In principle, it is possible to limit the right to be heard as well as other client rights, but there must be strong reasons for doing so. Urgency in itself is not a strong enough reason. The respective provisions of the Patent Act already limited the rights of the patentee, for example, by applying shorter timelines for decision-making, or immediate enforceability. In light of this, the HIPO should have recognised that any further limitation is against fundamental law principles. The patentee should have been provided the opportunity to fully defend its rights and interests at the HIPO, including adding context to the certificate on alleged unmet supply need issued by the pharmaceutical regulator. The formal possibility to appeal the HIPO decision cannot justify denying the patentee the possibility of being heard before the HIPO. The courts failed to identify the fundamental law aspects of the case and as a result did not remedy such flaws, so the court decisions are violating the fundamental rights to fair proceedings and to legal remedy. The lower courts focused on the time factor alone and refused to consider the patentee’s interests. This resulted in the patentee’s right to remedy becoming a mere formality. The Constitutional Court emphasized that the right to be heard as an essential element of client rights must be ensured in any proceedings. In this regard, the court referred to those recommendations of the Council of Europe which address this principle.

* 1. **Privacy**

In the case published under reference number BH 2017.1.20, the Hungarian Curia rendered a decision reflecting the case law of the Court of Justice of the European Union in the Bronner case[[85]](#footnote-85). The decision concerned the interpretation of point d) of Section 94(1) of the Copyright Act, which prescribes an obligation to provide information in case of infringement. The judgment is of fundamental legal importance as it emphasizes the primacy of personal data protection. The provision of information constitutes personal data processing, which is subject to strict conditions under data protection law. According to the judgment, profiling inferences drawn from IP addresses—based on internet usage and user habits—can be linked to a specific individual and pertain to the most intimate aspects of one’s personality. Such data may, in certain cases, even qualify as special categories of personal data, to which more stringent rules apply within the scope of personal data processing.

The decision stated: “*The data subject has a legitimate interest in ensuring that information concerning the characteristics of his or her personality is made public only based on his or her own decision or consent. At the same time, civil law enforcement, including the request for a service provider to disclose data, is not the exclusive remedy available to the party whose copyright has been infringed. Therefore, considering the above interests, there can be no doubt that the restriction of the right to the protection of personal data—which may in specific instances include special categories of personal data—is not proportionate to the enforcement interest stemming from copyright*.” On this basis, the court rejected the rightsholder’s request for the intermediary service provider to disclose the data.

We are not aware any cases of challenging the enforcement of intellectual property rights related to other fundamental rights.

* 1. **Outcome of the cases**

The outcomes demonstrate a consistent theme: Hungarian courts, guided by the Constitutional Court and the ECtHR, engage in a careful balancing act. The cases presented above raised legal issues originating from a similar constitutional context concerning the enforcement of intellectual property rights and fundamental rights, in particular the right to a fair trial and freedom of expression.

The central legal issue in the “Do not thread on Hungarians” case was whether the graphic and textual elements of the trademark violated the prohibition of public morality, which is a ground for exclusion from trademark protection. According to the HIPO and the courts, the trademark with the threatening text “...you'll get hurt!” goes beyond historical references and self-defense messages and contains a direct threat, thus violating public morality. The case highlights that freedom of expression is not unlimited, especially in an economic (trademark law) context, where other fundamental principles, such as the protection of public order and public morals may have priority.

The central legal issue in the “Szűztea” case was whether the right to a fair trial violated if no hearing were held in an extraordinary review process relating to a non-litigious procedure. According to the Constitutional Court, the right to a fair trial is not automatically violated by the fact that no public hearing is held if the type of proceedings, such as an extraordinary review, otherwise allows to omit a public hearing. The right to a fair trial does not require that personal appearance and a public hearing be guaranteed in all cases, especially in review proceedings against decisions made in non-litigious proceedings.

The lesson to be learned from these two cases is that fundamental rights, such as freedom of expression or right to a fair trial are balanced against other legal principles. These cases highlight the responsibility of the courts to take due account of substantive legal principles, such as procedural fairness and the freedom of expression in light of public morality and procedural guarantees like simplification and timeliness of the proceedings, as well as their completion within a reasonable time limit.

**Reflections**

1. **Assessment of current responsibilities and/or obligations of online platforms**

The current framework of responsibilities for online platforms in Hungary can be characterized as a complex, dual-layered system. At the legislative level, the adoption of the DSA has created a modern, sophisticated, and largely harmonized regime that establishes a clear, tiered system of obligations based on the nature and size of the intermediary service. The principles are clear: no general monitoring, conditional safe harbours, and enhanced due diligence for larger platforms.

However, at the level of practical enforcement, this clarity gives way to significant challenges and tensions. The most prominent of these is the structural conflict between the effective enforcement of intellectual property rights and the robust protection of data privacy. The Hungarian NTD procedure allows for swift initial takedowns, but its efficiency is crippled by the inability of rightsholders to identify anonymous infringers due to strict data protection interpretations by the courts. This leaves rightsholders with a remedy that is often procedurally potent but practically incomplete.

A second major tension exists between the DSA's principle of algorithmic transparency and the operational reality of opaque, AI-driven content moderation. Studies commissioned by the NMHH reveal that platforms' moderation practices remain a “black box,” and the redress mechanisms available to users are often ineffective against automated decisions. This suggests a significant gap between the rights granted to users on paper and their ability to exercise them in practice.

Finally, the division of enforcement labour—with private rightsholders driving IP cases, the HCA leading on unfair competition, and individuals pursuing other civil claims—creates a fragmented landscape of responsibility for platforms. Their obligations in practice are defined less by a single set of rules and more by the specific demands of the entity bringing a complaint.

1. **Foreseeable future developments and suggestions**

In the foreseeable future, major legislative upheaval is unlikely, as the focus for both platforms and regulators will be on the implementation and practical application of the new DSA framework. The guiding policy document for Hungary's digital future is the National Digitalisation Strategy 2022-2030, which aims to enhance digital infrastructure, competence, and the digital economy, aligning with the EU's “Digital Decade” goals.

Policy and enforcement trends will be the primary areas of development. The HCA is expected to continue its focus on the digital economy, with anticipated scrutiny of practices related to AI, greenwashing, and dark patterns. The NMHH, in its role as the Digital Services Coordinator, will be the central actor shaping the interpretation of the DSA in Hungary. Its future studies and the decisions of the out-of-court dispute resolution body (OPVT) will be critical in defining the practical contours of platform responsibility.

A significant factor shaping the future is the underlying political context. The Hungarian government has expressed concerns about what it perceives as politically motivated censorship by large platforms, particularly in relation to conservative viewpoints. Conversely, external observers and domestic opposition figures have voiced fears that the government could leverage its regulatory powers under the DSA to suppress critical speech. This political tension will inevitably influence how the NMHH exercises its considerable new powers. The future of platform regulation in Hungary will therefore be determined not only by legal interpretation but also by the navigation of this complex political landscape.

To enhance the legal landscape, a key suggestion would be to address the “enforcement black hole” in IP cases. This could involve creating a specific, narrowly defined legal procedure that allows rightsholders, upon presenting sufficient evidence of infringement to a court, to obtain an order for the disclosure of infringer identity data from intermediaries. Such a procedure would need to be carefully crafted with strong judicial oversight to balance IP enforcement with data protection rights, but it would address the most significant practical impediment to effective enforcement in the current system.

1. **Risk of automated filtering to fair dealing**

Under the CDSM Directive a new set of obligations has been put in place for online content-sharing service providers (OCSSPs). These entities are providers of information society services, who store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.[[86]](#footnote-86) Stemming from the above definition, these providers are a smaller group within the scope of the term ‘digital platforms’. As platforms giving access to copyright-protected works, the issue of filtering is vital in connection with their operation and the rights of copyright owners. In case of these platforms, it is safe to ascertain that they are handling huge amounts of copyright-protected materials. Therefore, the question of automated filtering inevitably arises. Under the CDSM Directive, it is forbidden to conduct general monitoring, i.e., which has also been in place since the E-Commerce Directive.[[87]](#footnote-87) However, the IPR Enforcement Directive[[88]](#footnote-88) states that ‘the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement’, the compliance with which obligation may only be verified through a kind of general monitoring. The CJEU has been dealing with automated filtering for a while now, and has long held the opinion that such automated filtering cannot lead to general monitoring, as it is contrary to the rules of the E-Commerce Directive, the InfoSoc Directive and the IPR Enforcement Directive, and is also in contradiction with several fundamental rights, such as freedom of expression, freedom to information, freedom to conduct a business and data protection.[[89]](#footnote-89)

In Hungary, fair dealing legislation has, in some part, an extensive history (e.g., quotation, education, personal use). In the other part, it is only present since the CDSM Directive. The modification complying with the CDSM Directive has entered into force on 1 June 2021. Criticism, review, quotation, parody, pastiche, and caricature have been added to the Hungarian Copyright Act, into Section 34/A. (1) a) and b). As per the reasoning behind the amendment of the Hungarian Copyright Act, Article 17(7) of the CDSM Directive mandated the implementation of the above exceptions into national legislation.

These instances of fair dealing, as agents of freedom of expression, need to be safeguarded against intrusion and conflict with other fundamental rights. In Hungary, when fundamental rights are in conflict, one has to be limited for the other to prevail. Limitation of fundamental rights in Hungary is conducted through a so-called ‘three-step test’. The steps are as follows: (i) is there a legitimate aim for the limitation; (ii) can the legitimate aim be achieved with this kind of limitation; and (iii) is the limitation and the legitimate aim proportionate to one another?[[90]](#footnote-90) If all three questions are answered with ‘yes’, a fundamental right may be limited in favour of another.

In case of automated filtering of content, the issue of overblocking due to false positive or false negative hits can lead to a limitation of freedom of expression, which in Hungary, as elaborated above, has to be subject to the above test. Furthermore, in case of automated filtering, it is unclear, how a system conducting such filtering can ascertain whether (i) the material in question has been uploaded or used rightfully, e.g., based on a license agreement; or (ii) it falls under fair dealing. *Mutatis mutandis* we refer to the Pelham decision of the CJEU, in which the Court had to decide whether the phonogram producer’s exclusive rights are infringed ‘if very short audio snatches are taken from its phonogram and transferred to another phonogram’.[[91]](#footnote-91) This case resulted in a preliminary decision of the CJEU, a lengthy procedure taking months.

However, it seems that we want automated filtering systems to make such decisions in the blink of an eye. And this is only a sample from a phonogram. In case of criticism, review and quotation we believe that the jurisprudence and legislation is quite clear, therefore establishing systems capable of recognizing these uses of otherwise protected subject matters is not as far-fetched, as it seemed a few years back. However, should we, can we and if yes, how can we expect such filtering systems to recognize the nuances of a parody, pastiche or caricature? The evolution of AI systems is a pathway to many abilities some consider to be unnatural. We can train AI systems to do our taxes, create motivation letters and Ghibli-style pictures of a family gathering. We can also ask ChatGPT to write us a sonnet about last night’s Champions League game in Shakespeare’s style. This may answer our questions regarding pastiche, as it has been able to (unknowingly maybe) create such works. But can we train it to have a sense of humour? What is humour anyway? The need to regulate caricature and parody seems to pose theoretical questions which may be answered by the CJEU or some form of EU legislation in the end.

Lastly, if it is possible to create such a system (most likely through the use of AI and machine learning), it would take a huge amount of preexisting works (caricatures, parodies, pastiches, reviews, quotations and criticisms) to feed and allow said filtering system to learn the rules of fair dealing, which are still unclear to human users in some cases. A further issue could be the need to adjust the system to national jurisdictions, which could mean further training data adapting to differences in legal systems, legislation and jurisprudence.[[92]](#footnote-92)

In conclusion, we refer to Professors Christophe Geiger and Bernd Justin Jütte, highly regarded scholars in the field of online copyright issues, who argue that the whole discussion regarding automated filtering stems from the misconception, that technology is able to solve all problems.[[93]](#footnote-93)

\*\*\*

1. Section 7 (2) and (4) of the E-Commerce Act (former version) [↑](#footnote-ref-1)
2. Section 7 (3) of the E-Commerce Act (former version) [↑](#footnote-ref-2)
3. Section 2 point l) of the E-Commerce Act (former version) [↑](#footnote-ref-3)
4. Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary App no 22947/13 (ECtHR, 2 February 2016, final 2 May 2016) [↑](#footnote-ref-4)
5. Magyar Jeti Zrt v Hungary App no 11257/16 (ECtHR, 4 December 2018, final 4 March 2019) [↑](#footnote-ref-5)
6. E-Commerce Act, Section 7 (1) [↑](#footnote-ref-6)
7. DSA, Article 3, point (g), (i) [↑](#footnote-ref-7)
8. DSA, Article 4 (1) [↑](#footnote-ref-8)
9. DSA, Article 3, point (g), (ii) [↑](#footnote-ref-9)
10. DSA, Article 5 (1) [↑](#footnote-ref-10)
11. DSA, Article 3, point (g), (iii) [↑](#footnote-ref-11)
12. DSA, Article 6 (1)-(3) [↑](#footnote-ref-12)
13. DSA. Article 6 (3) [↑](#footnote-ref-13)
14. DSA, Article 3, point (j) [↑](#footnote-ref-14)
15. Civil Code, Section 6:142 [↑](#footnote-ref-15)
16. Civil Code, Section 6:519 [↑](#footnote-ref-16)
17. DSA, Article 54 [↑](#footnote-ref-17)
18. Internet Intermediaries Act, Section 3 (2) [↑](#footnote-ref-18)
19. Internet Intermediaries Act, Section 3 (3) to (4) [↑](#footnote-ref-19)
20. Sections 12 to 14 of the Criminal Code [↑](#footnote-ref-20)
21. According to Article 23 (2) of Act on Business Advertising in connection with any infringement arising from the contents of advertising, the publisher of that advertising:

    a) shall be relieved from liability if treated as an intermediary service provider in accordance with Act CVIII of 2001 on E-Commerce, if in compliance with the requirements set out in Articles 8-12 of the E-Commerce Act;

    b) shall be held liable in the cases not regulated under Paragraph a) - with the exception set out in Paragraph c) - only if being able to study the contents of the advertisement; or

    c) shall not be held liable for the facts stated in advertisement materials addressed to unspecified recipients. [↑](#footnote-ref-21)
22. Notably, this understanding was expressly confirmed by the ministerial reasoning of Act XCIV of 2007 amending the E-Commerce Act. [↑](#footnote-ref-22)
23. <https://nmhh.hu/cikk/250507/A_mesterseges_intelligencia_donti_el_mi_a_tiltott_turt_es_tamogatott>. [↑](#footnote-ref-23)
24. DSA, Article 14 (1) [↑](#footnote-ref-24)
25. Regulation (EU) No 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC [↑](#footnote-ref-25)
26. Hungarian Competition Authority: Examining the impact of artificial intelligence on market competition and consumers. p. 28. [https://www.gvh.hu/pfile/file?path=/en/resolutions/sectoral\_inquiries\_market\_analyses/  
    market\_analyses/mesterseges-intelligencia\_piacelemzes\_hirdetmeny\_240104\_a&inline=true](https://www.gvh.hu/pfile/file?path=/en/resolutions/sectoral_inquiries_market_analyses/market_analyses/mesterseges-intelligencia_piacelemzes_hirdetmeny_240104_a&inline=true) [↑](#footnote-ref-26)
27. Is There a Free L(a)unch? Liability for Damages Caused by Interim Injunctions in Trademark Litigation in Hungary; Aron Laszlo (Oppenheim Legal)/December 17, 2020 <https://trademarkblog.kluweriplaw.com/2020/12/17/is-there-a-free-launch-liability-for-damages-caused-by-interim-injunctions-in-trademark-litigation-in-hungary/> [↑](#footnote-ref-27)
28. DSA, Article 22(2). [↑](#footnote-ref-28)
29. 7/2024. (VII. 31.) NMHH Decree. [↑](#footnote-ref-29)
30. Internet Hotline’s English language website: <https://english.nmhh.hu/internethotline/> [↑](#footnote-ref-30)
31. Internet Hotline Rules of Procedure: <https://english.nmhh.hu/article/245822/Rule_of_Procedure_of_the_Internet_Hotline#I._Definition_of_the_Internet_Hotline_> [↑](#footnote-ref-31)
32. See Article T)(2)-(4) of the Fundamental Law of Hungary. [↑](#footnote-ref-32)
33. See Article R) of the Fundamental Law of Hungary. [↑](#footnote-ref-33)
34. Pursuant to Article T)(3) of the Fundamental Law of Hungary “*No law may be contrary to the Fundamental Law.*” [↑](#footnote-ref-34)
35. As a brief side note, meanwhile the Constitutional Court of Hungary extrapolated the protection of IPR from the right to property based on Act XX of 1949 on The Constitution of the Republic of Hungary (“**Constitution**”), in light of the decision of the very same court, this extrapolation can be applied in connection with the Fundamental Law of Hungary. Pursuant to the enactment of the Fundamental Law, the Constitutional Court determined that it possesses the prerogative to employ the contentions articulated in its prior decisions, which were predicated on the provisions of the Constitution, in the adjudication of subsequent cases, provided that such contentions are deemed permissible in accordance with the specific provisions and interpretive principles of the Fundamental Law of Hungary, which provisions and principles are analogous to or congruent with those inherent in the Constitution. See Decision of the Constitutional Court of Hungary no. 22/2012 (V. 11.) AB point [40] and 13/2013. (VI. 17.) AB point [30]. [↑](#footnote-ref-35)
36. See decision 17/1992 (III. 30.) AB point 6. [↑](#footnote-ref-36)
37. See, in particular, decision 1338/B/1992 AB on patent rights. [↑](#footnote-ref-37)
38. See decision 3115/2013. (VI. 4.) AB point [35]. [↑](#footnote-ref-38)
39. See decision 3195/2016 (X. 11.) AB point [13] and decision 25/2015 (VII. 21.) AB point [55]. [↑](#footnote-ref-39)
40. „*The ownership of property shall entail social responsibility.”* [↑](#footnote-ref-40)
41. See decision 3232/2016. (XI. 18.) AB point [11] and decision 3150/2013. (VII. 24.) AB point [16]. [↑](#footnote-ref-41)
42. See decision 30/1992 AB point [2]. [↑](#footnote-ref-42)
43. In terms of the clear and present danger test see Schenck v. United States, 249 U.S. 47 (1919). In terms of actual malice test see New York Times Co. v. Sullivan, 376 U.S. 254 (1964). [↑](#footnote-ref-43)
44. See Article E)(3) and Q)(2)-(3) of the Fundamental Law of Hungary. [↑](#footnote-ref-44)
45. Announced by Act XXXI of 1993 on the proclamation of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on November 4, 1950, and its eight additional protocols. [↑](#footnote-ref-45)
46. By a quiet laconic way but Article 17(2) of Chapter II of the CFR states that “*Intellectual property shall be protected*”, leaving the *modus operandi* to the Member States. [↑](#footnote-ref-46)
47. Announced by the Act IX of 1998 on the proclamation of the Marrakesh Agreement establishing the World Trade Organization and its annexes, concluded within the framework of the General Agreement on Tariffs and Trade (GATT). [↑](#footnote-ref-47)
48. The Civil Code did not integrate industrial property rights and copyright laws, even though the subjective rights arising from intellectual property relations (and most of the sanctions for their infringement) are clearly of a private law nature. At the same time, in Section 2:55, the Civil Code emphasizes the private law nature of the protection of intellectual creations and other intellectual property, and therefore defines the background norms of its own rules in relation to the separate laws. [↑](#footnote-ref-48)
49. Act V of 2013 on the Civil Code (“**Civil Code**”). [↑](#footnote-ref-49)
50. Section 1:3 of the Civil Code. [↑](#footnote-ref-50)
51. Section 1:4 of the Civil Code. [↑](#footnote-ref-51)
52. Section 1:5 of the Civil Code. [↑](#footnote-ref-52)
53. Section 31 and 32 of PPI. [↑](#footnote-ref-53)
54. Section 15 of the Trademark Act. [↑](#footnote-ref-54)
55. Section 69 of the Copyright Act. [↑](#footnote-ref-55)
56. Section 68 of the Copyright Act. [↑](#footnote-ref-56)
57. Section 11 of the Trademark Act. [↑](#footnote-ref-57)
58. Section 18 of the Trademark Act. [↑](#footnote-ref-58)
59. Section 27/A of the Trademark Act. [↑](#footnote-ref-59)
60. Section 103 of the CCP. [↑](#footnote-ref-60)
61. See decisions 33/2015. (XII. 3.) AB point [13], 7/2015. (III. 19.) AB points [29]–[30], 6/2019. (III. 20.) AB point [20], 3284/2021. (VII. 7.) AB point [22]–[23]. [↑](#footnote-ref-61)
62. See Article XII of the Fundamental Law of Hungary. [↑](#footnote-ref-62)
63. See Article XIII of the Fundamental Law of Hungary. [↑](#footnote-ref-63)
64. See decision 8/2014. (III. 20.) AB point [61]. [↑](#footnote-ref-64)
65. See decisions 21/1994. (IV. 16.) AB point [2] and 59/1995. (X. 6.) AB point [1.1]. [↑](#footnote-ref-65)
66. Commission Regulation 2023/1067 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of specialization agreements, and its Hungarian counterpart Government Decree No. 467/2023 (X. 12.) on the exemption of certain groups of specialization agreements from the prohibition of competition restrictions. [↑](#footnote-ref-66)
67. Commission Regulation (EU) 2023/1066 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements and its Hungarian counterpart Government Decree No. 456/2023 (X. 5.) on the exemption of certain categories of research and development agreements from the prohibition of restrictions on competition. [↑](#footnote-ref-67)
68. Commission Regulation (EU) 2022/720 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices and its Hungarian counterpart Government Decree No. 306/2022 (VIII. 11.) on the exemption of certain categories of vertical agreements from the prohibition of restrictions on competition. [↑](#footnote-ref-68)
69. See Act LVII of 1996 on the Prohibition of Unfair Trading Practices and Unfair Competition (“**Hungarian Competition Act**”). [↑](#footnote-ref-69)
70. Act LVII of 1996 on the prohibition of unfair market practices and the restriction of competition (“**HCA**”). [↑](#footnote-ref-70)
71. Act XLVII of 2008 on the prohibition of unfair commercial practices against consumers (“**UCP Act**”). [↑](#footnote-ref-71)
72. Section 6 of the HCA. [↑](#footnote-ref-72)
73. Section 6/A of the HCA. [↑](#footnote-ref-73)
74. See decision of the Szeged Regional Court no. P. 21.305/2021/19. point [37]. [↑](#footnote-ref-74)
75. See decision of the Szeged Court of Appeal no. Pf. 20.147/2022/24. point [79]. [↑](#footnote-ref-75)
76. See decision of the Kúria Pfv.IV.20.914/2023/7. point [47]-[51]. [↑](#footnote-ref-76)
77. “Do not thread on Hungarians”. [↑](#footnote-ref-77)
78. See the decision of the HIPO M1802169. [↑](#footnote-ref-78)
79. The HIPO e-records is available on the following URL address: <http://epub.hpo.hu/e-nyilvantartas/?lang=HU> , case number: M1802169 (date of download: 12.05.2025.) [↑](#footnote-ref-79)
80. See the decision of the Budapest Metropolitan Court 1.Pk.20.670/2020.3. [↑](#footnote-ref-80)
81. See decision of the Metropolitan Court of Appeal Pkf. 25.411/2020/3. [↑](#footnote-ref-81)
82. “Virgin tea”. [↑](#footnote-ref-82)
83. See decision of the Kúria Pfv.IV.21.343/2017/4. [↑](#footnote-ref-83)
84. See the decision of the Constitutional Court 3251/2019. (X. 30.) AB. [↑](#footnote-ref-84)
85. Court of Justice of the European Union, Case C-461/10 – Bonnier Audio AB and Others v. Perfect Communication Sweden AB [ECLI:EU:C:2012:219] (2012) [↑](#footnote-ref-85)
86. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (hereinafter: CDSM Directive), Article 2(6) [↑](#footnote-ref-86)
87. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter: E-Commerce Directive), Article 15(1) [↑](#footnote-ref-87)
88. DIRECTIVE 2004/48/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 on the enforcement of intellectual property rights (hereinafter: IPRED Directive), Article 11 [↑](#footnote-ref-88)
89. cf. C-324/09. L’Oréal v. eBay, Opinion of AG Jääskinen; C-324/09. L’Oréal v. eBay; C-484/14. Tobias McFadden v. Sony Music Entartainement Germany GmbH, Opinion of AG Szpunar; C-70/10. Scarlet Extended v. SABAM; C-360/10. SABAM v. Netlog; C‑682/18. and C‑683/18. cases, YouTube/Cyando, Opinion of AG Øe; ; C‑682/18. and C‑683/18. cases YouTube/Cyando. [↑](#footnote-ref-89)
90. Fundamental Law of Hungary, Article I. (3) [↑](#footnote-ref-90)
91. C-476/17. Pelham 25(1) [↑](#footnote-ref-91)
92. In this regard we are aware of the issue of text and data mining, however, it falls outside of the scope of the present paper. [↑](#footnote-ref-92)
93. GEIGER, Christophe – JÜTTE, Bernd Justin: Platform Liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match. 2021, PIJIP/TLS Research Paper Series no. 64. (see [here](https://download.ssrn.com/21/05/25/ssrn_id3852687_code1952998.pdf?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEBUaCXVzLWVhc3QtMSJGMEQCIBQOiiMC3GiH7pztUtnMDkgFKASzOPnk%2BL230PZMV75XAiAVdPJUzZ3F0cx03g8hCYLJp1V1%2FS%2FKRVbLFcPlNM4nDirHBQiO%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F8BEAQaDDMwODQ3NTMwMTI1NyIMyRt6tN0sVJ2lShVdKpsFD5B%2BtP10PbN%2BzmngR9MLV9pIKbST05zL4TBaUEFt1qhaw%2FAwdNKo8Aa4rpLVniDslG4LPxuWcRQKtMInuFWVu7JHlDP6osmK1b%2BydJOvqWtoaji%2FtiYz%2B3j4hhQqGBdozjWrJujt032WGfCCVILzaNmuElHe3xrKOtcBisY%2BAd%2BQOrhFw3krIx9km657Foo2xNVr6rNSMMujtoG4f7OvXKtxktxDlFS0I1jmhqZCe%2BvdQAL1lBK8%2BcOUg4e8p08WNQBeDUOaSwys2BDib7pxGDTaT3YJk9iGiv9KN%2FpI1FnGpKhdP%2FReIqgkDqcOsYv%2BFn9ZmdlCEQjjyxNll9GX5PlgLvPs2cVzy54k15pGBJ%2FI34R%2BfTeiX38G4SBP6BoLOF7veCUxbBzyn9Q2Ob7VQ4iI09CdzTVXmMelQj6FaRc7Odr8kuacroVj5DWDTbDoNfxmksabPnLCJmV4oMTqSXIy%2Fldv%2BGXgzw5hBBbIM1XWz0NVXi%2Fi8ef81l2hOtN76W%2BV58Hxiwa1erP4dZl3xKfZDID4pm5%2BvcufbquCQTSm75sl36sqnZmq7O5c8vICx8Wa3KNy8Vg8WMppMykP37P%2BaFyeSI1OTEhhjr%2FpPE8Ny1NFLm5PNIm1TcYFWlqBBvWqyK4fwm3j%2BjI6Pk81UaHvT%2FfkflYOF1cOJRIH8vED%2BBS7OnlMdcWoWUz42HrnL23%2BR06y7KDjhQBQV%2BEezJ7WsxrR0t%2Fso2gt6UoEIq8fBfZwkvAlRvki4IRxZZypz%2BBmStA60FsyYHqXIgMHZSldrzQ7TcmBth7ypnKcksp6Tuk1r1lx6H4p43vJlMQTrR12ghzZfR1HWRr%2BdN%2B0D%2FKtAVKDqLLqyNxdYSzZw4X5JgXIxVkiUu1%2FSDCa2tm%2FBjqyAT2mQePWXERzlhZH3GXMrlu8L0aFGjiUUeXKVVjVa3eeYUspeuprX3Z%2F%2BcuSuSybqfpgmlGDl%2Fuab4Ht%2BMKLv34LGUNE5aSVSb5lm3l1S10q1a%2FSX0FeErRfN6MU8bnO2Tp7uaCFMarnHRGo49Cd2t7gdPjKGfPmZ7UBoLb9JtZVk5aoyE2nbLKxwuBZD%2Bir1cpOkhoX%2BZ9G4KTKXcPThWFszT%2B2Td7yZZqpob83BLog2Ns%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20250409T132719Z&X-Amz-SignedHeaders=host&X-Amz-Expires=300&X-Amz-Credential=ASIAUPUUPRWEQKKSON3H%2F20250409%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Signature=0752357a086113dd24a0f98943ff717aa411385e663c4d6626bbdc9788c9d533&abstractId=3776267)) [↑](#footnote-ref-93)