The presentation by Dr. Danguolė BUBLIENĖ,
the President of the Supreme Court of Lithuania,
delivered at the 2026 Conference of the Network of Presidents of the Supreme Courts of the EU (Limassol, Cyprus) presenting an overview of the case law of EU supreme courts on the application of the DSA.

Dear colleagues,

Over the past two decades, the Internet has evolved from a largely unregulated and peripheral space into a central infrastructure of modern life. It shapes how we communicate, work, access information, and even participate in democratic debate. Yet the legal framework governing the digital environment was created for a fundamentally different era. Not only smaller in scale, but also anticipating completely different challenges.

In fact, when the e-Commerce Directive was adopted in 2000, we could not yet imagine today's realities. Large-scale disinformation, algorithmic amplification, deepfakes, dark patterns, and the immense societal influence of online platforms are the products of modern times. But this is, in many ways, inevitable. Law tends to follow – or even lag behind – societal and technological change. This is especially evident in the digital sphere.

As the digital sphere expanded, so did the risks associated with it. Violations of privacy, misuse of personal data, manipulative online practices, and the rapid dissemination of illegal content exposed the limitations of the existing legal framework. It also highlighted the growing need for stronger protection of individuals' rights online. In response, the European Union adopted the Digital Markets Act and the Digital Services Act as part of a broader effort to shape Europe's digital future.

These acts came out together in 2022 as a nearly one-hundred-seventy-page legislative effort to establish harmonized rules for providers of intermediary services. In other words, rules "to control" the internet. Because of this, Europe may appear particularly strict in regulating the digital sphere. But in reality, governments around the world take different approaches to online regulation, defining obligations on online platforms, as well as the limits on their responsibility. These differences reflect deeper legal traditions, constitutional values, and political philosophies.

Authoritarian regimes often seek to maintain tight control over online content to preserve political power. Yet even among democratic states, there is no single model. The United States, traditionally a strong defender of freedom of expression, remains highly cautious about restricting speech online in any meaningful way. The United Kingdom, by contrast, places greater emphasis on online safety and risk prevention. The EU, meanwhile, seeks to strike a balance between the competing values and create a system that accommodates freedom of expression alongside a safer online environment.

The DSA, striving to create a safer and more transparent online environment, imposes obligations on online platforms relating to content moderation, transparency, complaint mechanisms, and the prevention of the dissemination of illegal content.

At the same time, it has opened a series of difficult legal questions. Perhaps the most important among them is how to protect users from what is online without undermining fundamental rights, particularly freedom of expression. This tension becomes even more acute as platforms increasingly rely on automated moderation and algorithmic systems to comply with their obligations.

The questionnaire that was prepared for our discussion covered key substantive and procedural issues likely to arise in the application of the DSA before national courts. A particular focus was placed on illegal content, platforms' obligations, users' remedies, and cross-border enforcement, in order to identify emerging challenges and potential divergences in national approaches. We received more than thirty responses, all of which will be made available in full by the Secretariat of the Network. I would like to thank the Presidents for creating this opportunity to explore and discuss these new issues in a comparative format.

However, the responses largely confirmed my initial concern that the topic, despite its novelty and significance, has not yet been developed extensively at the national level. In fact, many countries reported that they have not yet developed any judicial case law on the application of the DSA. Some of the questions remained unanswered, even at a hypothetical level. Many responses were based on the legal framework rather than on the established practice of its application. And finally, where the DSA was applied, it played a supporting rather than a central role. In practice, not only are private redress mechanisms mostly based on general provisions, but it seems that the DSA itself is not yet an act on which legal complaints and evaluations are directly based. These findings are not surprising – largely because the Regulation has not been in force long enough for disputes to emerge and progress through the national courts.

While it is difficult to identify common themes shared by *all* Members, we highlighted the areas where the greatest degree of convergence emerges. One such area is the concept of illegal content. Despite the absence of extensive and well-established case law, this issue attracted significant attention in your answers. It was, in fact, one of the questions that received the most responses.

What appears to be a problem is that the definition of illegal content is extremely broad. So broad, in fact, that it can appear almost circular. Put simply, illegal content is whatever is deemed illegal under EU or Member States' law. Yet this is where the complexity begins. The applicable laws may vary from one Member State to another. They are also interpreted through different legal traditions and enforcement frameworks, thus might expand along the way.

While some categories of content are widely recognized as illegal across jurisdictions, others are far more contested. For example, content related to criminal offences or trademark and copyright infringements is generally understood to fall within the scope of illegal content. It is also in line with the case law already developed under the e-Commerce Directive. Some other examples included unfair competition and unfair commercial practices, as well as consumer protection notions when an unsafe and prohibited product was listed on the online marketplace. Furthermore, the use of the DSA was also linked to political advertising content violating special electoral norms.

However, the legal status of some other categories may vary considerably from one jurisdiction to another. The case of surrogacy is a good example. As mentioned by our colleagues from France, advertising surrogacy services to French citizens would be regarded as unlawful under French law. Yet the same activity, particularly where it involves non-commercial or so-called "altruistic" surrogacy, would likely be viewed differently in countries such as Greece, Cyprus, or Portugal[1], where legal frameworks permitting altruistic surrogacy have been introduced. This contrast becomes even more pronounced when looking beyond the European Union. In countries such as Ukraine, surrogacy is an established legal and social practice. This shows that, despite the apparent simplicity of the concept, determining what constitutes illegal content often depends heavily on the legal, cultural, and regulatory context in which the assessment is made.

[1] Among the Member States, Ireland, Greece, Cyprus and Portugal have introduced legislation permitting altruistic surrogacy, but for some of these the legislation has not yet entered into force or further regulations are still missing. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769508/EPRS_BRI(2025)769508_EN.pdf

Another important observation highlighted in the Report concerns the relationship between illegal content and the adjacent concept of harmful content. In some jurisdictions, the notion of harmful content already plays a prominent role in the regulatory landscape. Against this background, and in light of the broader context of the DSA, it is possible that the distinction in the treatment of harmful and illegal content will become less evident.

This development raises important questions. As a matter of principle, harmful content and illegal content are distinct categories. Although the DSA does not define "harmful content", it covers a broader range of content that could harm society, including that which could harm children, incite violence, or promote disinformation. By contrast, "illegal content" generally covers such material as terrorist propaganda or child pornography, rather than mere insults, nudity, or provocations. They serve different regulatory purposes and, from the perspective of freedom of expression, should not necessarily lead to the same legal consequences.

Yet, in practice, the distinction may become blurred. Certain categories of harmful content may be subjected to restrictions that are functionally equivalent to those applied to illegal content. In other words, even if the legal classifications remain formally separate, the regulatory effect may be very similar. It can be questioned whether the DSA even puts in place appropriate safeguards enabling digital operators to implement such a nuanced approach. At the same time, this approach is unlikely to be shared uniformly across Europe – other jurisdictions may be far more reluctant to impose comparable restrictions on harmful content. As a result, significant differences in interpretation and enforcement may emerge between Member States.

Does it come as a big surprise? Given how broad and flexible the concept of illegal content is, it is rather a consequence of applying an open-ended concept across diverse national legal systems. Thus, the practical meaning and limits of the DSA will ultimately be determined not only by legislation but also by the courts tasked with applying it across the Member States. I believe that the Irish perspective on this question would be highly valuable for our discussion.

However, the concern that platform operators may over-remove content and thereby restrict freedom of expression seems, for now, to be more evident in theory than in practice. First of all, countries did not report examples in which a national court had concluded that the removal of a specific piece of online content constituted a violation of freedom of expression. This does not necessarily mean that concerns about over-removal are unfounded. However, it does suggest that, thus far, such concerns have rarely translated into judicial findings.

Second, colleagues from Germany shared an analysis by *Die Welt* on 70 million moderation decisions made by *Facebook, Instagram, TikTok*, and *X* in Europe in December 2025. They concluded that the DSA has not led to widespread over-censorship by platforms in Germany, and there was no evidence that platforms are removing legitimate content, thereby violating users' right to freedom of expression to a greater extent than before the DSA came into force. Also, according to the German Digital Services Coordinator, the preventive deletion of lawful content does not appear to be a widespread phenomenon. This is noteworthy, as such "over-removal" is often highlighted in academic discussions as a key concern regarding the DSA's potential impact on freedom of expression.

Lastly, it is worth noting that anyone can become a victim of what is shared online. In this respect, an interesting example comes from our colleagues from Slovenia.

Let me briefly share the essence of the story. A post on *X* by a prominent politician included a scan of a court ruling. In it, the personal data of several judges, including their names, identification numbers, and home addresses, were revealed. The post was followed by other posts in which other individuals disclosed the judges' places of residence and encouraged violence against them. In response, and to protect the judges and their personal data, the Supreme Court reported the content to *X* as illegal content.

Within a very short time – which suggests an automated response – the platform sent a message essentially dismissing the report and stating that the reported content was not found to be subject to removal under the legal grounds of DSA Law in the EU. A similar response followed after the appeal of the first response.

The matter was also brought to the attention of the responsible national agency (the Agency for Communication Networks and Services of the Republic of Slovenia) and the Information Commissioner. The European Commission was also contacted. Although no court proceedings were initiated, the disputed posts were removed within three days.

This suggests two interesting observations: first, the review process appears to rely heavily on automated, and likely artificial intelligence-driven, content assessment, rather than on a substantive review of the reported material itself. Second, the existing mechanisms do not seem to function as intended, as – most likely – only the European Commission's intervention led to a meaningful outcome. Finally, it remains unclear what actually triggered the removal of the content. It is not evident whether this was the result of a formal DSA-related framework or the broader influence of the European Commission. I believe that our Slovenian colleague Damjan

Orož (the President of the Supreme Court of Slovenia) will elaborate on this interesting experience and share more details of this case with us during the discussion.

Although our questionnaire did not include a specific question addressing similar situations, a real-life example illustrates how important this framework can be for *any* individuals and institutions alike. It also shows that existing mechanisms do not always function as intended, and that broader questions about protecting judges, as well as the integrity of the judicial system, other systemic risks may arise. Just a few days ago, Mis Laurence Pécaut-Rivolier (a member of the college of the French regulatory authority for audiovisual and digital communication (ARCOM), in her speech at the ENCJ event, stressed that online verbal violence has reached a new level, and that the justice system has become a special target in this environment. In her opinion, this has happened for at least two reasons.

First, because the justice system represents institutional authority, which is questioned and sometimes distrusted. Second, because political polarization can turn legitimate criticism of court decisions into personal attacks against judges. Such criticism can turn into public targeting. This may then lead to personal attacks, online harassment, or even threats.

Based on her personal experience and on several concrete examples, she encouraged further reflection on whether, beyond the tools that already exist, should the justice system develop a specialized mechanism – or even a dedicated trusted flagger – capable of quickly identifying coordinated harassment campaigns targeting judges and court staff online. She illustrated that in France, ARCOM has already started discussions with judicial and government authorities about the possibility of having an ARCOM accredited trusted flagger that could act when judges become specific targets online. This is not easy, but it is an important response. Similar work is already being done for journalists and elected officials.

If you have encountered comparable experiences, I invite you to share them during our discussion.

And finally – the current limited body of case law is not a sufficient indicator to definitively determine what we are observing. Whether it is the effective preventive impact of the DSA, or, on the contrary, uncertainties in its practical application that never reach courts.

Although Mr. Savvas Papasavvas will share his insights on the implementation of targeted internet supervision through the introduction of a tiered moderation system, and on rights protected by the DSA and procedural safeguards put in place, you may have noticed that I also proposed several additional questions at the end of the Report. They concern three issues: first,

whether the DSA will be interpreted and applied uniformly across the European Union and the role that national supreme courts will have in that. Second, whether the convergence between harmful and illegal content could risk leading to over-restrictions. And third, how judicial systems should adapt their remedies and responses when illegal content targets the courts themselves.

I believe these questions may at least help to forecast whether there are grounds to expect that the DSA will, over time, become an autonomous and directly applicable legal basis in judicial practice, or whether it will continue to function primarily as a contextual regulatory instrument.