

SEPTEMBER 14

2024

Weekend



Edition

N°198

REMY CHAVANNES AND KARLIJN VAN DEN HEUVEL

# THE PRE-EMPTIVE EFFECT OF THE DIGITAL SERVICES ACT



# The pre-emptive effect of the Digital Services Act

Remy Chavannes and Karlijn van den Heuvel <sup>1</sup>

The Digital Services Act ('**DSA**') has recently become applicable to intermediary service providers offering their services in the EU, from very large online platforms such as Facebook, Amazon and Booking.com to much smaller and less well-known digital service providers.<sup>2</sup> This landmark EU legislation aims to establish a fully harmonised framework for intermediary services to ensure a safe, predictable and trusted online environment. Given the full harmonisation aim, the question arises how much room there is left for national legislation in this field. Despite the DSA's detailed rules, Member States may still perceive a need to address specific domestic concerns, for example in relation to the protection of minors or disinformation. This Long Read examines to what extent the DSA pre-empts such national laws, exploring what (if any) competence remains for Member States.

## 1. Preliminary: the ECD's country of origin principle

Before discussing the pre-emptive effect of the DSA, we should point out another important limit on Member States' power to regulate online intermediary services: the country of origin ('**COO**') principle included in the Directive on Electronic commerce ('**ECD**').<sup>3</sup> The DSA does not affect applicability of this principle, which applies to all information society services, including the intermediary services which are regulated by the DSA.<sup>4</sup>

The ECD's COO principle essentially states that the Member State in which an information society service provider ('**ISSP**') is established, has both the right and the duty to regulate that provider in accordance with its national law.<sup>5</sup> All other Member States must allow the service in their territory without imposing their own additional (limiting) rules in the coordinated field. They may not restrict an ISSP from another Member State, except if they comply with the substantive and procedural requirements set out in the derogation mechanism in Article 3(4) ECD, which is interpreted strictly.

1. The authors are lawyers in the EU platform regulation & litigation practice at a law firm in Amsterdam. They regularly advise clients in the digital media and technology fields on issues such as those discussed in this contribution, but the views expressed are their own personal opinions.

2. [Regulation \(EU\) 2022/2065](#) of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ 2022 L 277, p. 1).

3. [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 (Directive on electronic commerce) (OJ 2000 L 178, p. 1).

4. Art. 2(3) DSA.

5. Art. 3 ECD.

Recent judgments from the Court of Justice have further strengthened this COO principle. The Court has first clarified that it is not possible to derogate from the COO principle with measures of a general and abstract nature that are aimed at a generally described category of providers.<sup>6</sup> In other words, a generally applicable law cannot be used to derogate from the COO principle. Only measures directed at a given – specified, individualised – ISSP are allowed. Secondly, the Court of Justice has clarified that a legitimate derogation from the COO principles requires a direct link with one of the purposes for which the ECD allows a derogation.<sup>7</sup> National measures which are likely, at best, to have only an indirect link with those objectives, cannot form a legitimate derogation from the COO principle, also where these measures are intended to ensure adequate and effective enforcement of EU law.<sup>8</sup>

These judgments affirm both the significance of the ECD's COO principle and the restrictive nature of the derogation mechanism. Member States do not always seem sufficiently aware of this important limit on their legislative power. For example, a recent Italian legislative initiative to protect minors online contains obligations directed at providers of information society services that offer their services in Italy, regardless of their place of establishment.<sup>9</sup> We would argue that this clearly violates the ECD's COO principle, which is in line with various detailed opinions from the European Commission in response to TRIS notifications of national laws with a similar scope of application.<sup>10</sup>

The COO principle can be a source of tension because it removes Member States' ability to legislate, also in relation to issues which are important to their domestic politics, instead requiring them to place their trust in the regulations and enforcement infrastructure in the Member State of establishment

6. [Judgment of the Court of Justice of 9 November 2023](#), *Google Ireland and Others* (C-376/22, EU:C:2023:385).

7. Art. 3(4)(a)(i) ECD.

8. [Judgment of the Court of Justice of 30 May 2024](#), *Airbnb and Amazon and Google and Eg Vacation Rentals* (Joined cases C-662/22, para 83 and C-667/22, para. 86).

9. Article 1 of [the proposed Italian bill for the protection of minors in the digital dimension](#).

10. [Notification 2024/0188/DE](#), Detailed Opinion, p. 4-5; [Notification 2024/0002/HU](#), Detailed Opinion, p. 4-5; [Notification 2023/554/IT](#), Detailed Opinion, p. 3-4; [Notification 2023/461/FR](#), Detailed Opinion, p. 2-3.

The COO principle can be a source of tension because it removes Member States' ability to legislate, also in relation to issues which are important to their domestic politics, instead requiring them to place their trust in the regulations and enforcement infrastructure in the Member State of establishment. That Member State of establishment has often been Ireland – at least in the case of globally operating technology companies – and the perceived limitations of Irish enforcement were an important reason for the Council to amend the DSA to place enforcement of compliance by very large platforms in the hands of the European Commission. Beyond the DSA's obligations directed at very large online platforms however, the COO principle remains in force, and Irish legislation and enforcement continue to have a major influence on online services throughout the EU.

## 2. The concept of pre-emption

Pre-emption is a concept or legal doctrine to indicate that Member States are precluded from adopting or maintaining national laws on account of EU law. Understood as a rule of competence, pre-emption means that the exercise of EU competence blocks the exercise of national competence.<sup>11</sup> This is most clearly reflected in Article 2(2) TFEU on shared competence. Other scholars interpret the concept of pre-emption as a rule of conflict, which determines whether the laws of a Member State conflict with EU law.<sup>12</sup> Irrespective however of whether pre-emption is seen as a rule of competence or a rule of conflict, the outcome is the same: Where a Member State strays into pre-empted territory, the national rules must be disapplied in accordance with the principle of primacy.

To determine the pre-emptive effect, the level of harmonisation that an EU regulation seeks to achieve is key. Where EU law exhaustively regulates a certain field, intending full (or maximum) harmonisation, there is not much (or any) room left for Member States to regulate the same issues under national law. By contrast, minimum harmonisation goals do leave room for Member States to take additional national measures. The pre-emptive effect is therefore most profound in cases of full harmonisation.

## 3. The full harmonisation goal of the DSA

Article 1 DSA states that the aim of the regulation is to 'contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment' and that it 'lays down harmonised rules on the provision of intermediary services in the internal market'. The intention for the DSA to be a *full* harmonisation instrument is apparent from Recital 9, which states that (emphasis added):

11. Timmermans, C. (2014) '[ECJ Doctrines on Competences](#)' in Azoulai, L. (ed) *The Question of Competence in the European Union*, Oxford University Press, p. 159.

12. Robert Schütze, '[Supremacy without pre-emption? The very slowly emergent doctrine of community pre-emption](#)', *Common market law review* 43(4), 2006, p. 1030; Amadeo Arena '[Exercise of EU Competences and Pre-emption of Member States](#)' *Powers in the Internal and External Sphere: Towards 'Grand Unification?'* *Yearbook of European Law*, 46(1), 2016, p. 32.



*‘[t]his Regulation fully harmonises the rules applicable to intermediary services in the internal market with the objective of ensuring a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated.’*

The reason for the DSA’s harmonising intent – and indeed justification – is set out clearly in Recitals 2 and 4 (emphasis added):

*‘Member States are increasingly introducing, or are considering introducing, national laws on the matters covered by this Regulation, imposing, in particular, diligence requirements for providers of intermediary services as regards the way they should tackle illegal content, online disinformation or other societal risks. Those diverging national laws negatively affect the internal market [...]*

*[...] in order to safeguard and improve the functioning of the internal market, a targeted set of uniform, effective and proportionate mandatory rules should be established at Union level. [...] The approximation of national regulatory measures at Union level concerning the requirements for providers of intermediary services is necessary to avoid and put an end to fragmentation of the internal market and to ensure legal certainty, thus reducing uncertainty for developers and fostering interoperability.’*

**Because the DSA is a full harmonisation instrument, Member States are precluded from maintaining or introducing national requirements for intermediary service providers relating to issues regulated by the DSA, except where this is explicitly provided for by the DSA**

Because the DSA is a full harmonisation instrument, Member States are precluded from maintaining or introducing national requirements for intermediary service providers relating to issues regulated by the DSA, except where this is explicitly provided for by the DSA. Member States are additionally not precluded from introducing laws that pursue other legitimate interest objectives than the DSA. This can be again found in Recital 9 (emphasis added):

*‘Accordingly, Member States should not adopt or maintain additional national requirements relating to the matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of the fully harmonised rules applicable to providers of intermediary services in accordance with the objectives of this Regulation. This should not preclude the possibility of applying other national legislation applicable to providers of intermediary services, in compliance with Union law, including Directive 2000/31/EC, in particular its Article 3, where the provisions of national law pursue other legitimate public interest objectives than those pursued by this Regulation.’*

This full harmonisation effect of the DSA has also been repeatedly emphasised by the European Commission in recent responses to TRIS notifications of various national laws (emphasis added):<sup>13</sup>

*'The Commission recalls that, being a Regulation, the DSA does not allow for additional national requirements unless otherwise expressly provided. This is because, pursuant to Article 288 TFEU, regulations are directly applicable throughout the Union. Unlike in the case of directives, national implementing measures are therefore not permitted in relation to regulations, unless the regulation itself leaves it to the Member States to adopt the necessary legislative, regulatory, administrative and financial measures to ensure the effective application of the provisions of that regulation. The DSA neither requires nor permits that Member States adopt additional national requirements, unless otherwise expressly provided, in relation to the subject matter covered by it. This is emphasised in recital 9 of the DSA.'*

Against this background, it is quite clear that a national law that falls within the (broad) scope of the DSA will quickly stray into pre-empted territory. Given the full harmonisation goal of the DSA, this is arguably not only the case where the national law (directly) conflicts with the rules set out by the DSA, but also where the national law imposes *additional* requirements on intermediary service providers with the same objective as the DSA. In this latter case, Member States are precluded from imposing requirements on intermediary service providers with the (broad) objective of ensuring a safe online environment, because the DSA already exhaustively regulates this field.

The pre-emptive effect of the DSA may become more disputed in areas where the DSA does not set out detailed requirements or no requirements at all. In those cases, Member States may wish to impose stricter or more detailed requirements than the DSA provides. Based on the full harmonisation goal of the DSA, it can however be argued – as explained in the previous paragraph – that the DSA *exhaustively* regulates the entire regulatory field and that Member States are precluded from adding to this framework. Simply put, where the EU legislator has chosen *not* to regulate, this choice should be respected. This seems especially clear for rules that were rejected after consideration in the DSA's legislative process, but arguably applies more broadly.



13. [Notification 2023/759/LT](#), Detailed Opinion, p. 4-5. Similarly: [Notification 2024/2/HU](#), Detailed Opinion, p. 6; [Notification 2024/188/DE](#), Detailed Opinion, p. 6-7.

**Where the EU legislator has chosen *not* to regulate, this choice should be respected.**

**This seems especially clear for rules that were rejected after consideration in the DSA's legislative process, but arguably applies more broadly**

## 4. The pre-emptive effect of the DSA

In this section, we will attempt to further delineate the pre-emptive effect of the DSA by looking more closely at its substantive provisions. The DSA's rules can be divided in three categories: (i) intermediary liability exemptions, (ii) due diligence obligations, and (iii) implementation and enforcement.

### 4.1 Intermediary liability exemptions

The DSA maintains the existing intermediary liability framework that originates from the ECD. Under the so-called 'safe harbours', which are conditional liability exemptions, intermediary service provider cannot be held liable for illegal content provided by a recipient of the service. This applies in relation to any type of liability as regards any type or illegal content, irrespective of the precise subject matter or nature of those laws. The DSA replaces the safe harbours from the ECD, requiring Member States to repeal their national transpositions of the ECD's safe harbours.

From a pre-emption perspective, it seems clear that Member States cannot introduce or maintain rules which hold an intermediary service provider liable for illegal content whilst satisfying the conditions for a liability exemption under the DSA. Similarly, Member States cannot introduce additional conditions for application of the safe harbours. Such national rules would directly contravene the DSA and we would therefore argue that they are pre-empted by the DSA.

*For example:* The French LCEN creates criminal liability for providers of hosting services that do not comply with an obligation to promptly inform the competent authorities about illicit activity on their service that qualifies as certain criminal offences under French law (which are listed by the law) and which has been reported to them by recipients of the service.<sup>14</sup> This provision would be pre-empted if it would hold the provider liable, criminally or otherwise, in relation to user-uploaded content whilst it meets the conditions for the safe harbour.

14. Article 6(IV)(A) of [French Law No. 2005-575 on confidence in the digital economy](#).

*For example:* The draft Irish Gambling Regulation Bill requires that ‘a person’ shall not include, or cause to be included, a sample game in an advertisement of a relevant gambling activity, subject to a fine and imprisonment.<sup>15</sup> To the extent applicable to providers of intermediary services, which is not entirely clear, this seems pre-empted by the DSA, because these providers cannot be held liable for information provided by recipients of the service (in this case, a gambling advertisement including a sample game) where they meet the conditions of a safe harbour.

Whilst national laws that undermine the safe harbours seem clearly pre-empted by the DSA, Member States remain free (within the limits of EU law) to decide what constitutes illegal content, for example in national criminal law.<sup>16</sup> Similarly, the safe harbours do not affect the possibility to issue orders to terminate or prevent an infringement.<sup>17</sup> The DSA does not provide the legal basis for such orders nor regulates their territorial scope or enforcement, but merely harmonises specific minimum requirements for the content of the orders.<sup>18</sup> For this reason, pre-emption seems less likely. It remains to be seen, however, how the minimum requirements interact with national law. Although ostensibly impacting only the obligation to *inform* national authorities of the effect given to the order as required under article 9 and 10 DSA, these requirements could turn out to affect the validity of orders under national law. Some Member States already follow this interpretation, as demonstrated by the Greek and Maltese DSA implementing laws.<sup>19</sup>

## 4.2 Due diligence obligations

The bulk of the DSA sets out a catalogue of due diligence obligations for providers of intermediary service providers. These obligations take a tiered, asymmetrical approach, depending on the type of intermediary, with the least obligations applicable to mere conduit and caching services, and more obligations applying to hosting services, including (very large) online platforms. We will discuss these obligations in three categories. First, due process requirements for content moderation. Second, other due diligence requirements. Third and last, additional obligations for very large online platforms and very large search engines (together referred to as ‘**VLOPs**’).

### 4.2.1 Due process requirements for content moderation

An important part of the DSA sets out a detailed and comprehensive framework for content moderation by hosting providers and online platforms, requiring transparency in terms of service, a mechanism for notifying illegal content, and appeals (Articles 14-24 DSA). It is therefore difficult to see how Member States could introduce or maintain any due process requirements for content moderation that are not pre-empted by the DSA, notably including more stringent turnaround times.

---

15. Art. 143(3) of [the Irish Gambling Regulation Bill \(version passed by Lower House\)](#).


16. Art. 3(h) DSA defines ‘illegal content’ as content that is not in compliance with EU law or any Member State law which complies with EU law’.

17. Art. 4(3), 5(2) and 6(4) DSA.

18. Art. 9 and 10 DSA, see also recital 31 DSA.

19. Art. 12 and 13 of [Greek Law 5099/2024](#); Art. 5(1) and 6(1) of the [Maltese Digital Services \(Designation and Enforcement\) Order, 2024](#).





**It is therefore difficult to see how Member States could introduce or maintain any due process requirements for content moderation that are not pre-empted by the DSA, notably including more stringent turnaround times**

*Example:* Various national laws that served as blueprint for the DSA contained more detailed due process rules that did not end up in the DSA. The German NetzDG and the Austrian Kopl-G for instance required that online platforms removed illegal content within a specific 24 hours (or 7 day) timeframe after receiving a notice.<sup>20</sup> In the legislative process of the DSA, specific turnaround times were rejected, instead conditioning the safe harbour on that the hosting provider must ‘act expeditiously’ to remove or disable access to the illegal content.<sup>21</sup>

#### 4.2.2 Other due diligence requirements

Besides the content moderation requirements, the DSA contains a host of due diligence requirements applicable to intermediary service providers (Articles 11-13, 25-32 DSA). This is a somewhat miscellaneous catalogue of requirements, including requirements on single point of contact, transparency, advertising, recommender systems, protection of minors, and traceability of online traders. Some of these obligations apply to all intermediaries and others to hosting providers, online platforms and online marketplaces. The pre-emption argument in relation to these obligations is, in our view, threefold.

First, it seems obvious that Member States may no longer impose obligations on intermediary services that in some form conflict with or undermine the obligations of the DSA.

---

20. Art. 3(3) of the [Austrian Communications Platforms Act](#); Art. 1(3) of the German Network Enforcement Act (both no longer in force).

21. Amendment 111 of the [Opinion of the Committee on Legal Affairs](#) for the for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council on Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

*Example:* The German Interstate Media Treaty requires media intermediaries (i.e. search engines, video sharing platforms, and app stores) to designate an authorised recipient in Germany, whereas the DSA only requires extra-EU intermediaries to appoint a legal representative in the EU (Article 13 DSA).<sup>22</sup>

*Example:* Despite the clear harmonising intent of the DSA to allow providers to set a *single* point of contact, there are several examples of national laws that set additional or diverging requirements from Article 11 DSA. For example, the Danish DSA Implementation Act allows the Minister to require that written communication to and from competent authorities about matters covered by the DSA must take place digitally and by making use of specific IT systems, special digital formats and digital signatures.<sup>23</sup> Other examples can be found in Italy<sup>24</sup>, Germany<sup>25</sup> and France.<sup>26</sup>

*Example:* The French LCEN includes a list of criminal offenses that must be notified to the relevant authorities under Article 18 DSA.<sup>27</sup> To the extent these are not, as Article 18 DSA requires, criminal offenses ‘involving a threat to the life or safety of a person or persons’, this seems to be pre-empted by the DSA.

Second, we would argue that the DSA also pre-empts national laws that upset the asymmetrical system of due diligence obligations under the DSA. Not all due diligence obligations are applicable to all types of intermediary services. Arguably, Member States are therefore precluded from adopting more strict requirements for certain categories of services, thereby ‘promoting’ them to a regime that they do not fall in under the DSA.

*Example:* In Spain, online platforms and online search engines are required to collect certain information about advertisers of financial instruments before publishing their advertisements.<sup>28</sup> Under the DSA, know-your-customer requirements however only apply to online platforms allowing consumers to conclude distance contracts with traders (online marketplaces). In that sense, the Spanish law upsets the balance of the DSA by ‘promoting’ other types of intermediaries to a stricter regime, which is arguably pre-empted by the DSA.

22. Article 92 of the [German Interstate Media Treaty](#) (*Medienstaatsvertrag*). Art. 5 of the (repealed and no longer in force) [Austrian KoPl-G](#) contained a similar obligation.

23. Art. 15 of the [Danish Act on the enforcement of the Regulation of the European Parliament and of the Council on an internal market for digital services](#).

24. Article 144-bis(6) of the [Italian Privacy Code](#).

25. Section 92 of the [German Interstate Media Treaty](#).

26. Art. 6-4(2) [French Law No. 2005-575 on confidence in the digital economy](#) (which has been repealed by the [French Law No. 2024-449 aimed at securing and regulating the digital space](#)).

27. Article 6(IV)(A) of the [French Law No. 2005-575 on confidence in the digital economy](#).

28. Art. 246(3) of the [Spanish Financial Services Ads Law](#).

Third and last, it can be argued that the DSA *exhaustively* regulates all due diligence obligations for intermediary service providers in the sense that it is a complete catalogue of requirements for a safe online environment, thereby pre-empting any other national requirements applicable to providers of intermediary services that pursue the same aim, even if they do not necessarily conflict with the DSA. Under this field pre-emption approach, Member States may not pursue *any* further legislation in this area, even if it complements DSA rules or where there is no overlap with the substantive rules of the DSA, because the regulatory field has been exhaustively regulated. This would mean, for example, that Member States cannot impose additional requirements on intermediary service providers relating to the protection of minors or disinformation. In our view, there is good support for this position based on Recital 9 and Article 1(2)(b) of the DSA.

*Example:* The Italian proposal for an Online Child Safety Bill contains specific measures that online platforms must take to protect minors online. This includes implementing age verification for larger online platforms according to standards established by Italian regulator AGCOM, implementing a functionality to directly activate the Italian child emergency number 114, and verifying compliance with specific labour law requirements for (in short) commercial child influencers. Even though the DSA does not set such detailed rules, these requirements can still be seen as conflicting with the DSA, which allows the online platform to decide which measures are appropriate and proportionate (Article 28 DSA) and specifically requires VLOPs to take targeted measures to protect the child as measures to mitigate risks, including age verification and parental control tools aimed at helping minors signal abuse or obtain support where appropriate (Article 35(1)(j) DSA). The same argument can be made against the German Youth Media Protection State Treaty, which has also been pointed out by the European Commission,<sup>29</sup> and the French decree aimed at strengthening parental control over means of accessing the Internet.<sup>30</sup>

**It can be argued that the DSA exhaustively regulates all due diligence obligations for intermediary service providers in the sense that it is a complete catalogue of requirements for a safe online environment, thereby pre-empting any other national requirements applicable to providers of intermediary services that pursue the same aim, even if they do not necessarily conflict with the DSA**

29. [Notification 2024/188/DE](#), Detailed Opinion, p. 6-7.

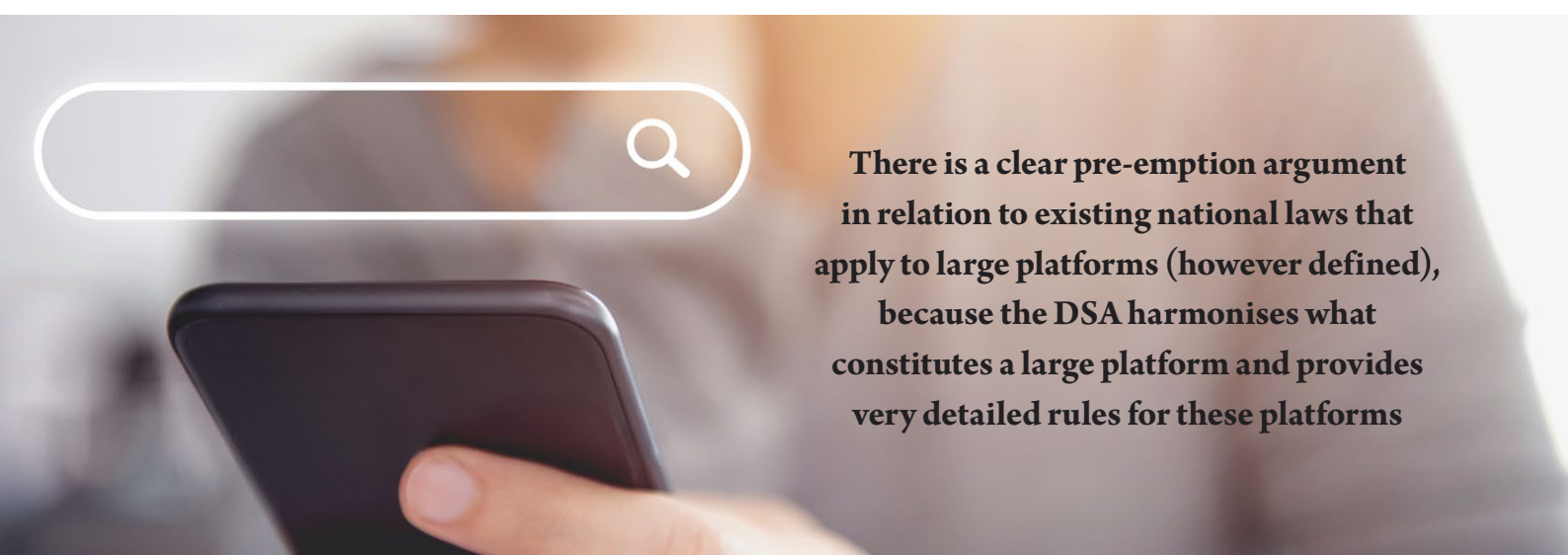
30. [French decree No. 2023-588 of July 11, 2023 taken for the application of Article 1 of Law No. 2022-300 of March 2, 2022 aimed at strengthening parental control over means of accessing the Internet.](#)

*Example:* The Irish Electoral Reform Act requires online platforms to put in place a notice and action mechanism for notification of disinformation, misinformation and manipulative or inauthentic behaviour in respect of online electoral information.<sup>31</sup> It also requires additional transparency reporting on disinformation.<sup>32</sup> These obligations add to the framework established by the DSA, which requires a notice and action mechanism for the notification of illegal content and transparency reporting on content moderation. The Irish requirement is arguably pre-empted by the DSA, because the DSA does not only aim to address illegal information online, but also the societal risks that the dissemination of disinformation or other content may generate (Recital 9). Since the DSA does not explicitly allow Member States to set additional rules, Ireland seems precluded from doing so.

#### 4.2.3 VLOP obligations to assess and mitigate systemic risks

The DSA introduces a harmonised set of diligence obligations specifically applicable to very large online platforms and very large online search engines (together referred to as ‘VLOPs’) in relation to the assessment and mitigation of systemic risks (Articles 33-43 DSA). The European Commission is exclusively competent to enforce these rules.<sup>33</sup>

There is a clear pre-emption argument in relation to existing national laws that apply to large platforms (however defined), because the DSA harmonises what constitutes a large platform and provides very detailed rules for these platforms, with supervision and enforcement centralised at the European Commission. This harmonised approach would be undermined if Member States would maintain or adopt parallel regimes for very large platforms, or impose VLOP-like obligations on services which are not designated as VLOPs.

A hand holding a smartphone is shown in the foreground. A white search bar with a magnifying glass icon is overlaid on the screen. The background is blurred, showing a person's face.

**There is a clear pre-emption argument in relation to existing national laws that apply to large platforms (however defined), because the DSA harmonises what constitutes a large platform and provides very detailed rules for these platforms**

31. Art. 149(1), (2) and (3) of the [Irish Electoral Reform Act](#).

32. Art. 149(5) and (6) of the [Irish Electoral Reform Act](#).

33. Art. 56(2) DSA.



*Example:* The Irish Electoral Reform Act requires online platforms with over 1 million unique monthly users in Ireland, as early as possible in an election campaign period, to prepare and transmit a risk report to the Electoral Commission. Arguably, the harmonising intent of the DSA is undermined if Member States start using alternative thresholds to determine ‘national VLOPs’. Substantively, the Irish rules very much overlap with the risk assessment and mitigation framework of Articles 34-35 DSA, which also covers electoral processes, and therefore seem pre-empted.

### 4.3 Implementation and enforcement

The DSA is directly applicable and in principle does not require national implementing measures. One area in which the DSA does require implementation is supervision and enforcement, which is largely entrusted to national authorities. The DSA requires Member States to designate one or more competent authorities, one of which should be made the Digital Services Coordinator (‘DSC’), and sets out their powers and maximum fines. The DSA therefore clearly does not pre-empt national laws that designate such authorities and their investigatory and enforcement powers.

Member States should however not maintain or introduce provisions that go against the harmonised system of the DSA. In particular, the DSA sets out a clear division of competences. The Member State in which the main establishment of the provider of intermediary services is located has exclusive powers to supervise and enforce the DSA. Similarly, the European Commission is exclusively competent to supervise and enforce rules specifically applicable to very large online platforms. National laws that cut across this division of competences therefore seem pre-empted.

*Example:* The draft version of the French SREN law entrusted the enforcement of the notified provisions to the French authorities alone, including with regard to service providers outside the jurisdiction of France. The European Commission called upon France to bring this in conformity with the DSA’s supervision and enforcement structure.<sup>34</sup> The enacted version of this law in our view still includes overbroad enforcement powers, granting French regulator Arcom the power to collect information (necessary for requests under Article 58 and 65 of the DSA) from any intermediary service provider that offers their service in France.<sup>35</sup>

Additionally, copy-pasting of DSA obligations in national laws can also undermine the DSA’s enforcement mechanism. Although the obligation would remain the same, making it a national provision could result in enforcement by a national regulator that is not actually competent to enforce the obligation under the DSA.

The DSA furthermore harmonises the investigative and enforcement powers of national authorities. It therefore appears that Member States may not grant powers beyond the already broad powers set out in the DSA and must observe the maximum fines.

34. [Notification 2023/461/FR](#), Detailed Opinion from the European Commission, p. 5.

35. Article 51(5°) of [French Law No. 2024-449 aimed at securing and regulating the digital space](#).

**The DSA furthermore harmonises the investigative and enforcement powers of national authorities. It therefore appears that Member States may not grant powers beyond the already broad powers set out in the DSA and must observe the maximum fines**

*Example:* Under the French SREN, non-compliance with (the French implementation of) article 18 DSA is punishable by a fine and imprisonment.<sup>36</sup> Similarly, the Greek DSA implementing law allows punishment with imprisonment for whoever obstructs or hinders an investigation.<sup>37</sup> The catalogue of enforcement powers under the DSA does not include imprisonment, which is therefore arguably pre-empted.

## Conclusion

In this contribution we have analysed to what extent Member States still have room to regulate online intermediary services. Recent case law has affirmed and strengthened the COO principle in the ECD, leaving little room for Member States of destination to regulate intermediary service providers established in another Member State. Moreover, our analysis demonstrates that the DSA, as a full harmonisation instrument, curtails the freedom of all Member States to impose further regulations on intermediary service providers with the aim of ensuring a safe, trusted and predictable online environment.

We conclude that many of the Member State laws discussed in this contribution are likely pre-empted by the DSA. Leaving such laws in place would, in our view, run counter to the harmonising intent of the DSA, increasing rather than decreasing fragmentation in the digital single market, and increasing the complexity and uncertainty that the DSA was intended to reduce. In this complex legal landscape, we see a role for both the European Commission to intervene as well as for providers of intermediary services to challenge these laws before national courts.

36. Article 48(1)(5<sup>o</sup>), specifically the new Art. 6.-IV-A, of

37. Art. 44(7) of [Greek Law 5099/2024](#).



**Permission to use this content must be obtained from the copyright owner**

**All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.**



**Editor-in-Chief:**  
Daniel Sarmiento  
.....

**In-Depth and Weekend Edition Editor**  
Sara Iglesias Sánchez  
.....

**Editorial Board:**  
Maja Brkan, Marco Lamandini, Adolfo Martín, Jorge Piernas, Ana Ramalho,  
René Repasi, Anne-Lise Sibony, Araceli Turmo, Isabelle Van Damme,  
Maria Dolores Utrilla and Maria Weimer.

**Subscription prices are available upon request. Please contact our sales department for further information at**

subscriptions@eulawlive.com

ISSN

EU Law Live **2695-9585**  
EU Law Live Weekend Edition **2695-9593**

EU  
LAW  
LIVE

