
CEPS EXPLAINER

# UNPACKING THE FEDIVERSE

## What it is, why it matters – and how it could cause a major headache for the DSA

Paula Gürtler

2025-02

## SUMMARY

With the growing number of users on alternative social media platforms, such as Threads, Mastodon and Bluesky, the notion of 'federated' platforms and how legal frameworks apply to them are becoming a pressing issue. This CEPS Explainer dives into two characteristics of federated platforms in light of the EU's Digital Services Act (DSA) – decentralisation and federation.

While all user accounts on traditional social media are hosted on a central server by one organisation, accounts on federated platforms (that make up the 'fediverse') resemble email accounts, in the sense that one can choose whether to create a Gmail, Hotmail or Yahoo account but they can still send emails to any other account because the underlying protocols are interoperable. In the fediverse, users can decide between different 'instances' – servers or communities – hosted by all kinds of organisations. The rules and administration of content moderation are 'federated' and managed by the instance hosts. Overall, there isn't one singular decentralised social network. There are many different communities across instances on different services (e.g. Mastodon, Threads) that are in turn connected to one another. This means that content can be (and is) shared across platforms and services.

The DSA applies to fediverse services and characterises each instance as a platform. But there are two pressure points in applying the DSA to the fediverse: i) the decentralisation of server hosts results in a number of small organisations hosting instances, which means that exempting small and micro enterprises could lead to compliance gaps; and ii) the federation of services makes it more difficult on how to count the active users of services, since content is able to spread beyond one service and across platforms, thus potentially over- or underestimating the systemic risk of fediverse platforms.

This Explainer advocates that federated platforms need to engage closely with the DSA and work together on a strategy to ensure compliance. On top of this, the methodology for classifying VLOPs needs to be revisited so that the systemic risk of federated platforms can be accurately evaluated and then the responsibility for mitigating said risk is properly assigned.



Paula Gürtler is an Associate Researcher in the Global Governance, Regulation, Innovation and Digital Economy (GRID) unti at CEPS.



CEPS Explainers offer shorter, more bite-sized analyses of a wide range of key policy questions facing Europe. Unless otherwise indicated, the views expressed are attributable only to the authors in a personal capacity and not to any institution with which they are associated.

© CEPS 2025

# INTRODUCTION

The Digital Services Act (DSA), fully applicable since 17 February 2024, has had an impressive first year. It has made headlines around the world as the European Commission opened formal proceedings against X, TikTok, and AliExpress. The DSA is celebrated as a landmark achievement in how to regulate digital intermediary services and online content moderation, and it's widely regarded an example of ambitious law making. We now need to look towards the future to make sure that it has many more impressive years ahead of it.

The DSA calls on platforms to enhance the mechanisms for removing illegal content and aims to effectively protect users' fundamental rights online, including their freedom of expression. It also creates stronger public oversight over online platforms by mandating systemic risk assessment, establishing transparency obligations, addressing issues like dark patterns and algorithmic recommender systems, and mandating that 'vetted' researchers can access key data and algorithms.

But even an enlightened and innovative piece of legislation like the DSA might not stand the test of time. Its future-proofness might be put to the test by the next-generation of social media platforms, so-called federated social media services, also known as 'fediverse' services.

The most widely known services in the fediverse are Mastodon, Threads and Bluesky. In the months after Elon Musk bought Twitter, these services have seen a spike in new user accounts, leading many experts to predict that they'll come to dominate the social media landscape, eventually sucking in all frustrated Twitter fans who are uneasy about being on X.

Although it's a little early to draw conclusions about this ongoing trend, it makes sense to already ponder whether the DSA would still be fit for purpose if the fediverse becomes the 'new normal' for social networks in the years to come.

# WHAT IS THE FEDIVERSE? AND WHY IS IT IMPORTANT?

At first glance, fediverse services might not look too different from centralised social media platforms[1]. Users have a personalised feed where different content can be seen – images, articles, short text posts etc.[2]. However, what makes fediverse services different from more 'traditional' social media platforms is that this feed is typically not algorithmically curated but highlights the content of users who are registered on the same server you are, or accounts that you follow on other servers and across different services.

This means that there are two key characteristics of the fediverse – first, the possibility to host accounts on different servers (i.e. decentralisation) and second, interoperability between platforms (i.e. federation)[3].

## A DECENTRALISED WORLD

If one creates a social media account, this account is registered on a server. In Facebook's case, all Facebook accounts are registered on a server owned and controlled by Meta. It's the same with TikTok and all other centralised social networks. Their key features are (i) a single authority (i.e. the server owner takes all decisions about the platform's functionality, data handling and governance), (ii) central data storage, i.e. all user data, content and interactions are stored on a single company's servers, giving the company full access and control over how this data is used; (iii) the company that owns the platform and servers governs (normally through algorithms) content moderation, user bans and enforcing community standards; and finally (iv) the platform owner controls how advertisements are displayed, targeted and monetised.

The fediverse is different. When one opens an account on a fediverse service, the process resembles more that of creating an email account. One can choose whether to open an account with Gmail, Hotmail, Yahoo etc. and no matter which one is chosen, emails can still be sent to any other account and the email account can be used to subscribe to services or mailing lists – because the underlying protocols (POP, IMAP, and SMTP) are all interoperable.

---

[1] It's important to note that there are still many technical challenges to be overcome regarding fediverse services. This Explainer deals with the fediverse as imagined in its ideal state, while fully accepting that the current reality might still be two steps behind.

[2] There are sub-feeds, though, that e.g. for Mastodon can be distinguished into the 'local' feed, which highlights the activity of users who are registered on the same server. On the 'home' feed users can see posts from users that they follow across Mastodon servers (and eventually also on other fediverse platforms like Threads).

[3] Overall, the fediverse is typically characterised by five aspects: decentralisation, federation, user autonomy, privacy and data ownership, and the lack of a central authority. This Explainer focusses on decentralisation and federation specifically in the context of the DSA.

Decentralised social networks rely on an open activity protocol (ActivityPub in Mastodon and Threads' case). Users don't choose between email providers but between servers where their account will be hosted. A server is a node in the federated system and is called an 'instance'. If one registers on the Mastodon social instance (the biggest one yet and the default when you download the app) the user's account would be *@name@Mastodon.social*. If one chooses to register on the 'Climate Justice' instance, your account handle could be *@name@climate_justice*.

In principle, all instances using the Activity Pub protocol can interact with each other. Thus, content posted from one account on one instance can be seen, liked, shared or reposted by an account registered on another server.

However, the choice of instance matters quite a bit. It determines who holds your account data and who's responsible for providing the hosting services, which includes continuous availability and guaranteeing cybersecurity. Each instance has its own 'homepage', its own community, its own rules and is run by different people. Crucially, the rules and content moderation are federated and managed by the instance owner, i.e. an independent administrator.

**Table 1.** Summary of differences between traditional social media and fediverse services

| Traditional social media | Fediverse services |
|---|---|
| Central authority. | Instance administrators and decentralised open-source activity protocol. |
| Centralised data storage. | Data storage with instance hosts. |
| Centrally managed content moderation, user bans, community standards. | Community-based content moderation. |
| Centralised control of how ads are displayed, targeted, and monetised. | No ads and algorithmic feed. |

*Source:* Authors' own elaboration.

Overall, there isn't one singular decentralised social network. There are many different communities across instances on different services that are in turn connected to one another. The content on a user's personal feed doesn't necessarily all originate from the same service. For example, the feed on a fediverse platform could integrate content from a microblogging service such as Mastodon and Threads, as well as videos form 'PeerTube', and you can interact with all this different content from your own instance. In short, this means that content is shared *across* platforms and services.

In theory, user accounts should be able to move seamlessly between instances and platforms. For example, if *user@Mastodon.social* disagreed with a decision taken by the

instance administrator, they can simply move their account to another instance on any platform at any time while *keeping* their followers, for example becoming *user@Climate_Justice*[4]. This mechanism aims to avoid the concentration of power and lock-in effects for platform users, emphasising the appeal of interoperability to empower users. While the technical solutions for some of these features are still being worked in, we can already anticipate some challenges when it comes to the DSA.

## THE DIGITAL SERVICES ACT – INNOVATIVE BUT IS IT FUTURE-PROOF?

The DSA, which fully entered into force in February 2024, holds online platforms and very large online platforms (VLOPS) responsible for the consequences of their operations, imposing on them several transparency and accountability requirements. VLOPs are defined as those online platforms that count more than 45 million monthly active users in the EU. Following a risk-based approach, obligations imposed by the DSA become more demanding for VLOPs (and Very Large Online Search Engines, or VLOSE), which are presumed to pose 'systemic risks'. The additional obligations for VLOPS are:

- To identify the risks to fundamental rights that their service poses and implement mitigation measures.
- To allow researchers to access platform data when the research contributes to the detection, identification and understanding of systemic risks in the EU. Researchers can access data either for vague explorative research (Article 40(12)) or apply for 'vetted researcher' status which gives them authorised access (Article 40(4)).
- To grant users the right to personalise content recommender systems, including giving them the option that what they see on their feed isn't based on profiling.
- To pay an annual supervisory fee to the Commission.
- To conduct an audit by an independent auditor at least once a year and adopt measures that respond to the auditor's recommendations.

All this means that the DSA marks a true paradigm shift when dealing with online platforms. Imposing responsibility on online intermediaries was previously considered taboo, also as a corollary of the 'net neutrality' principle. In the internet's original design, intermediaries were not expected to inspect content flowing between users and thus couldn't be made responsible for any consequences. This soon changed as the internet

[4] At least this is the *vision* of fediverse developers – the real technical implementation still has a way to go. The fediverse community is currently working on building apps that offer similar uses/features but are interoperable and decentralised.

became a mass phenomenon and when new large-scale platforms started monitoring traffic and drawing enormous profits from doing so.

However, the DSA also has a potentially fatal flaw. It implicitly assumes that regulated online platforms are centralised. *Decentralised* platforms may not be easily captured by provisions that are based on single entities managing their network through a single authority, with centralised data storage and content moderation, and with centralised control of advertising. Algorithm Watch has warned, for example, that '*the people who wrote the DSA clearly did not have the fediverse in mind. They spent no time discussing non-commercial social networks*.'

But whether the co-legislators did or did not consider the fediverse, the DSA still applies to fediverse instances nonetheless.

## THE FEDIVERSE AND THE DSA – DOES THE SHOE FIT?

As intermediary service providers, fediverse instances fall within the DSA's scope. More specifically, individual fediverse Instances should be classified as hosting services, or even online platforms[5]. After all, they provide access to server space (hosting service) and users are encouraged to share, like and interact with information hosted on individual instances (i.e. the online platform).

Additionally, they are responsible for content moderation, which is subject to the DSA. The lack of consideration given to the fediverse leads to a pretty awkward situation – while individual instances are possibly covered by the DSA, the overarching actors in the fediverse that provide a user interface, such as Mastodon and Threads, seem to fall between the cracks[6].

Overall, there are at least two 'pressure points' when the fediverse finds itself being squeezed into the DSA, related to *decentralisation* and *federation* as defining features of fediverse platforms.

[5] Intermediary services include mere conduit, caching and hosting services, as well as online platforms and VLOPS. For an overview on the various definitions in the DSA, see here.

[6] It's worth highlighting here that Mastodon is more decentralised compared to BlueSky and Threads, representing in a way the archetypical federated service. While BlueSky and Threads in theory allow for decentralisation, in practice, most accounts are hosted on the same server. This means that the challenges discussed in this Explainer are most pressing for Mastodon. BlueSky is already actively working on complying with the DSA. As a Meta service, Threads is finding itself under much more scrutiny.

## Decentralisation – pressure point or compliance challenge?

With the individual instances within the fediverse classified as online platforms, their ability – and also the necessity for them – to comply with the DSA becomes much more important.

**While fediverse services might reduce polarisation problems relative to centralised platforms, users belonging to marginalised communities have also reported 'levels of racist abuse unseen on commercial platforms', thus demonstrating how important it is that the DSA applies to fediverse instances.**

The hosting organisations behind instances are very different kinds of entities, ranging from Mastodon itself, to the German data protection authority, to small groups of activists. As with any EU regulation, 'proportionality' was considered in the DSA, which ultimately led to micro and small enterprises being exempted under Article 19 for some of the more demanding obligations. While fediverse services might reduce polarisation problems relative to centralised platforms, users belonging to marginalised communities have also reported 'levels of racist abuse unseen on commercial platforms', thus demonstrating how important it is that the DSA applies to fediverse instances. The size of the organisation hosting an instance doesn't necessarily correspond to the level of the instance's systemic risk, which relates to its overall reach.

For example, *@Mastodon.social*, run by Mastodon GmbH, a small enterprise, had approximately 2.3 million registered accounts as of January 2025, making it the largest Mastodon instance. Exempting Mastodon GmbH and other instance-hosting organisations due to Article 19 doesn't appear to be the ideal solution to tackle platforms' systemic risk and the prevalence of harmful and illegal online content, especially as the number active user numbers is poised to grow across instances.

As already mentioned, each instance has its own content moderation rules and is responsible for enforcing them. This is often done by community moderators and rarely involves algorithmic filters. Even without the DSA, keeping up with content moderation has been a challenge for larger instances run by small organisations. Since users of one instance can also seamlessly interact with content on another instance, situations can occur where one instance fails to act on harmful or illegal content, thus making it visible to users on another instance. While moderators can block other instances, the offending content from that instance remains online.

This is why some additional structures should be considered to coordinate the moderation of illegal content across multiple fediverse servers – which, indeed, is very much an idea that runs counter to the fediverse's decentralisation principle.

### FEDERATION AS A PRESSURE POINT – THE NUMBER OF 'AVERAGE MONTHLY ACTIVE RECIPIENTS'

Another issue which can already be predicted for when the DSA is being applied to the fediverse lies in the counting of active users and the threshold for VLOPs. Recital 77 of the DSA provides more insight into the methodology for counting active users of digital services. It reads:

> *'… the number of average monthly active recipients of an online platform should reflect all the recipients actually engaging with the service at least once in a given period of time, by being exposed to information disseminated on the online interface of the online platform.' (Recital 77)*

While this appears to be easily applicable to centralised platforms, transferring this word-for-word over to the fediverse is not such an easy task and will prove challenging.

For example, a post made by a user on the instance *@Climate_Justice* might be seen and liked by ten users on *@Mastodon.social* and then 10 users of *@threads.net*. Are these users now counted as 10 users of *@Mastodon.social* and 10 users of *@threads.net* or are they 20 users of *@Climate_Justice* or are they both? After all, they're being exposed to and are engaging with a *@Climate_Justice* post but they did so via their feed on the Mastodon and Threads Instances.

Should it matter then that these are accounts on different fediverse services? And which platform would be the origin of the 'systemic risk' here? And should that platform thus be subjected to additional obligations under the DSA?

Intuitively, it appears to make most sense to count users according to the platform that they're registered on. In this example, this means that there are 10 users on *@Mastodon.social* and 10 users of *@threads.net* and one user on *@Climate_Justice* (who originally posted).

However, it's the content moderation practices of *@Climate_Justice* that determines whether the post stays up or gets deleted *permanently* from the ActivityPub protocol. The Mastodon and Threads instances can block the content or even any communication from the *@Climate_Justice* instance – but crucially it remains searchable to users if they simply switch to another instance.

Considering the DSA's Recital 77, the above example can also be interpreted so that the users of fediverse platforms should actually be counted multiple times – in our example, we have 20 users engaging with the *@Climate_Justice* post, meaning that they're engaging with this platform's content and can be considered as active *@Climate_Justice*

users. But they're also engaging with the Mastodon and Threads instances, making them active users of these platforms. Counted this way, our example has now ballooned to 40 active users.

But counting users of fediverse platforms multiple times may lead to an overestimation of the systemic risk that fediverse platforms pose. In our example, it's actually only 20 people involved – not 40. The risk of over-counting active users is thus problematic for fediverse platforms because it raises proportionality questions. Depending on which platform these users are counted for, the additional obligations for VLOPS would come into play, which also includes paying the annual supervisory fee to the Commission, as set out in the DSA's Article 43.

On the other hand, if they are counted only for the instance which they are registered with, being classified as a 'VLOP' can be avoided indefinitely by users purposely coordinating with each other. Since the instance where a user registers matters less than for centralised social media, users can spread out across instances to purposely remain under the VLOPs threshold. Crucially, the possibility for seamless interaction between instances means that systemic risks can't be assessed by only looking at one instance in isolation.

This is why the DSA could be badly equipped for federated structures that do not have a single central authority that can ultimately be held responsible.

To conclude, the DSA doesn't give a clear answer on how to count active user accounts and how to mitigate potential systemic risks from fediverse platforms, which of course challenges its overall effectiveness. Due to the ongoing process to implement the full federation of fediverse services, the systemic risk will need to be estimated differently.

To square this circle, the Commission should wield its power to implement delegated acts on how active users are counted in a way that recognises and accounts for the emergence of fediverse platforms. Alternatively, there should be a review over whether federated platforms need to adjust their fundamental structure and operating principles, considering that they may generate systemic risks otherwise – perhaps not today, perhaps not tomorrow, but it's certainly possible in the near future considering their continued growth.

## ENSURING A TECHNOLOGY-NEUTRAL DSA

The main question is of course – what now? The DSA is in force and applicable. Harmful content is shared on federated platforms just as consistently as on centralised social media platforms. There's absolutely no reason why the fediverse should not pose a similar systemic risk as user numbers keep growing.

Nonetheless, most hosting organisations of fediverse instances – that should be classified as online platforms – fall under Article 19's exemption. And yet this Explainer clearly shows that the fediverse is possibly going to be a major headache for the DSA. The counting of active users on these platforms is sure to become an issue *eventually* and would be best addressed pre-emptively with some clear guidance at EU level.

**BOTH THE DECENTRALISATION OF CONTENT MODERATION AND THE NON-PROFIT BUSINESS MODEL ARE CORE IDEALS OF THE NEW GENERATION OF SOCIAL MEDIA PLATFORMS THAT ARE NOT ACCOUNTED FOR BY THE DSA**

The first pressure point outlined above suggests that federated platforms need to engage closely with the DSA and work together on a strategy to ensure their compliance. Both the decentralisation of content moderation and the non-profit business model are core ideals of the new generation of social media platforms that are not accounted for by the DSA. A dialogue between fediverse instance hosts and regulators could be initiated to find a solution. Concretely, the Commission could convene a taskforce that includes diverse stakeholders, ranging from organisations that offer fediverse services, consumer advocates like BEUC, and researchers familiar with user behaviour and the systemic risks of fediverse services.

The second pressure point suggests that the methodology for classifying VLOPs needs to be revisited to capture the systemic risk of federated platforms and distribute the responsibility as appropriate. Concrete steps that can be taken by the Commission are, for example, initiating a study (including multiple stakeholder inputs) to reflect further over how to apply the threshold to fediverse platforms or even to launch an open stakeholder consultation.

But the message is clear – if the Commission wants to have a future-proof DSA that can effectively respond to multiple future iterations of social media platforms, then they need to start paying close attention to the fediverse *now*.

CEPS
Place du Congres 1
B-1000 Brussels