









# DIGITAL SERVICES ACT: LIBE PLENARY AMENDMENTS V8 (17 JAN)

## Table of Contents

 1. PROTECTING DIGITAL PRIVACY & THE RIGHT TO ANONYMITY.....	2
 2. LIMITING GOVERNMENT SURVEILLANCE OF ONLINE ACTIVITY.....	3
 3. NO ACCESS BLOCKING .....	4
 4. REMOVAL ORDERS TO BE ISSUED BY COURTS ONLY .....	5
 5. WHAT IS LEGAL OFFLINE SHALL STAY UP ONLINE .....	6
 6. ENSURING THE FREE EXCHANGE OF LAWFUL INFORMATION AND MEDIA CONTENT ONLINE.....	8
 7. BRINGING UPLOAD FILTERS IN LINE WITH FREE SPEECH AND MEDIA FREEDOM .....	9
 8. MY TIMELINE, MY CHOICE.....	10

# 1. PROTECTING DIGITAL PRIVACY & THE RIGHT TO ANONYMITY

In recent years, numerous data breaches have exposed users' personal information, such as phone numbers and locations, to criminals. These breaches could have been avoided if users data was not unnecessarily gathered. **The Digital Services Act should provide for the right to use and pay for digital services anonymously** wherever reasonably feasible, in line with the principle of data minimisation and in order to prevent criminal activity, unauthorised disclosure, identity theft and other forms of abuse of personal data.

**Use case:** In 2021, 533 million Facebook users' private phone numbers (including those of MEPs) were published on a hacker forum. Facebook had collected these numbers unnecessarily. The data facilitates crime and exposes users to risks of SIM swap and phishing attacks as well as stalking.

## PAST EP RESOLUTIONS:

### [EP Resolution 2020/2018\(INL\)](#), par. 37:

"...unless required by specific legislation otherwise, intermediaries of digital services should enable the anonymous use of their services to the maximum extent possible..."


### [EP Resolution 2020/2019\(INL\)](#), par. 18:

"Stresses that in line with the principle of data minimisation and in order to prevent unauthorised disclosure, identity theft and other forms of abuse of personal data, the Digital Services Act should provide for the right to use digital services anonymously wherever technically possible; ..."

## PLENARY AMENDMENTS TABLED BY LIBE:

### [PLENARY AMENDMENT 517](#) – TO MERGE WITH IMCO AMENDMENT 25


Recital 28

 In accordance with the principle of data minimisation and in order to prevent unauthorised disclosure, identity theft and other forms of abuse of personal data, recipients should have the right to use and pay for information society services anonymously wherever reasonable efforts can make this possible. This should apply without prejudice to the obligations in Union law on the protection of personal data. Providers can enable anonymous use of their services by refraining from collecting personal data regarding the recipient and their

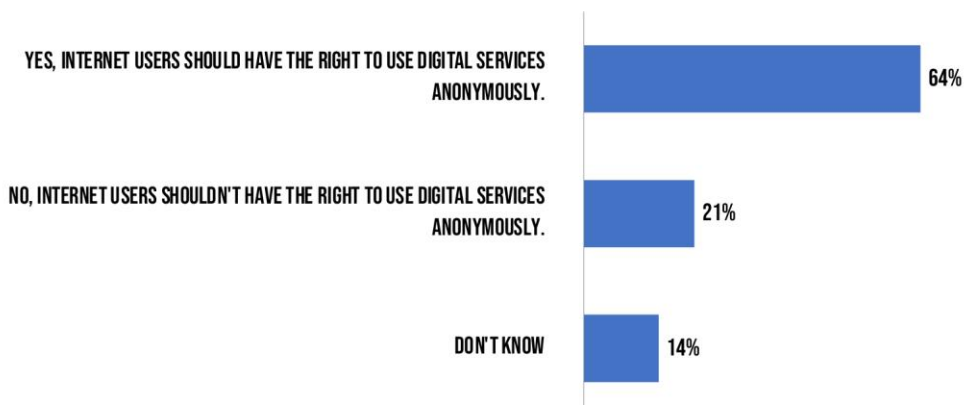
online activities and by not preventing recipients from using anonymizing networks for accessing the service. Anonymous payment can take place for example by paying in cash, by using cash-paid vouchers or prepaid payment instruments.

### [PLENARY AMENDMENT 520](#)

Article 7 – paragraph (new)

 Without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC, providers of intermediary services shall make reasonable efforts to enable the use of and payment for that service without collecting personal data of the recipient.

## RIGHT TO USE THE INTERNET ANONYMOUSLY



## 2. LIMITING GOVERNMENT SURVEILLANCE OF ONLINE ACTIVITY

In the spirit of the [case law on communications metadata](#), public authorities shall be given **access to records of personal online activity only to investigate suspects of serious crimes or prevent serious threats to public safety with prior judicial authorisation**. The fact that a person uses a certain digital service can be very revealing regarding their private life, religion, health or sexuality. The disclosure of such information can result in harassment or blackmailing. Also identifying an anonymous account can expose a whistleblower and result in serious harm. These limitations shall not apply to administrative authorities seeking to identify traders.

**Use case:** In Poland government (administrative) authorities allegedly used spyware to monitor prominent opposition figures, a lawyer and a prosecutor. Data requests on the basis of the new Digital Services Act without judicial authorization could also be abused for political purposes.

### PAST EP RESOLUTIONS:

#### [EP Resolution 2020/2018\(INL\)](#), par. 25:

"Stresses that, in the spirit of the case-law on communications metadata, public authorities shall be given access to a user's subscriber data and metadata only to investigate suspects of serious crimes with prior judicial authorisation;"



#### [EP Resolution 2020/2019\(INL\)](#), par. 19:

"stresses that in line with the case law on communications metadata, public authorities must be given access to a user's metadata only to investigate suspects of serious crime and with prior judicial authorisation;"

### PLENARY AMENDMENTS PROPOSED BY LIBE:


#### [PLENARY AMENDMENT 531](#) – TO MERGE WITH IMCO AM 160

##### Article 9 - paragraph 1

Providers of intermediary services shall, upon receipt of an order to provide a specific item of information about one or more specific individual recipients of the service, issued by the relevant national judicial  ~~or~~ **administrative** authorities on the basis of the applicable Union or national law, in conformity with Union law,  **for the purposes of preventing, investigating, detecting and prosecuting serious crime or preventing serious threats to public security inform** without undue delay the authority of issuing the order of its receipt and the effect given to the order.

#### [PLENARY AMENDMENT 532](#)

##### Article 9 - paragraph 2.a (new)

 **the order is issued for the purpose of preventing, investigating, detecting and prosecuting serious crime or preventing serious threats to public security;**


#### [PLENARY AMENDMENT 533](#)

##### Article 9 - paragraph 2 .a.a (new)

 **the order seeks information on a suspect or suspects of serious crime or of a serious threat to public security;**


#### [PLENARY AMENDMENT 534](#)

##### Article 9 - paragraph 2 - point a - indent 1 a (new)

 **a unique identifier of the recipients of the service on whom information is sought;<sup>1</sup>**


#### [PLENARY AMENDMENT 535](#)

##### Article 9 - paragraph 4 b (new)

 **This Article shall apply, mutatis mutandis, in respect of competent administrative authorities ordering online platforms to provide the information listed in Article 22 for other purposes than those set out in paragraph 1.<sup>2</sup>**

#### [PLENARY AMENDMENT 536](#)

##### Article 9 - paragraph 4 c (new)

 **Providers of intermediary services shall disclose personal data on recipients of their service requested by public authorities only where the conditions set out in this Article are met.<sup>3</sup>**

1 To prevent bulk data requests on unspecified users.  
2 Limitations not to apply to administrative authorities seeking to identify traders. When it comes to the effective investigation of commercial activities, it appears justified to apply lower safeguards.

3 Effectively harmonise conditions and safeguards for government access to personal data by preventing Member States from circumventing Article 9.

### 3. NO ACCESS BLOCKING

Mere conduit intermediaries should not be required to block access to content. **Illegal content should be removed where it is hosted.** Access blocking leaves content online and therefore can easily be circumvented (e.g. by changing DNS servers) and often results in overblocking and collateral suppression of legal speech hosted on the same website, by the same provider or via the same network (IP address).

**Use case:** In 2020 Italy blocked access to the digital library Project Gutenberg, essential for educational and research activities. Even though only small parts of the library allegedly violate Italian Copyright laws (these works are in the public domain in the US), access to the entire website has been blocked by the Italian authorities.

#### PAST EP RESOLUTIONS:

[EP Resolution 2020/2018\(INL\)](#), par. 49:

*"underlines that illegal content should be removed where it is hosted, and that access providers shall not be required to block access to content;"*


[EP Resolution 2020/2022\(INI\)](#), par. 16:

*"Underlines that illegal content should be removed where it is hosted, and that mere conduit intermediaries should not be required to block access to content;"*

#### PLENARY AMENDMENTS PROPOSED BY LIBE:

##### [PLENARY AMENDMENT 522](#)

Article 3 - paragraph 3

 ~~This Article shall not affect the possibility for a judicial or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.~~



## 4. REMOVAL ORDERS TO BE ISSUED BY COURTS ONLY

To protect freedom of expression and media freedom, **the decision on the legality of content shall rest with the independent judiciary**, not with administrative authorities. Suppressing online speech interferes with fundamental rights and requires a balancing of interests, which is typically entrusted to independent courts. **Administrative authorities are controlled by the government whereas the judiciary is generally shielded against politically motivated interference.** This corresponds to recommendations i.e. in the Joint Declaration on International Mechanisms for Promoting Freedom of Expression of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression. However, in view of the reduced risk to freedom of expression, administrative authorities should have the right to have unlawful commercial offers by traders removed.

**Use case:** A French administrative authority in 2019 requested the US digital library “Internet Archive” remove the content of hundreds of URLs which did not, as alleged, contain “terrorist propaganda”, but have high scholarly and research value, for example government-produced broadcasts.



### PAST EP RESOLUTIONS:

[EP Resolution 2020/2019\(INL\)](#), par. 5:

*“considers that the final decision on the legality of user-generated content must be made by an independent judiciary ...”*



### PLENARY AMENDMENTS PROPOSED BY LIBE:

#### [PLENARY AMENDMENT 523](#)

##### Article 4 - paragraph 2

This Article shall not affect the possibility for a court ~~- or~~ **administrative authority**, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

#### [PLENARY AMENDMENT 524](#)

##### Article 5 - paragraph 4

This Article shall not affect the possibility for a court ~~- or~~ **administrative authority**, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

#### [PLENARY AMENDMENT 525 – TO MERGE WITH IMCO AM 143](#)

##### Article 8 - paragraph 1

Providers of intermediary services shall, upon the receipt of an order to act against a specific item of illegal content, issued by the relevant national judicial ~~- or administrative~~ authorities, on the basis of the applicable Union or national law, in conformity with Union law, inform the authority issuing the order of the effect given to the orders, without undue delay, specifying the action taken and the moment when the action was taken.

#### [PLENARY AMENDMENT 526](#)

##### Article 8 - paragraph 1 - subparagraph 1 a (new)

**+ This Article shall apply mutatis mutandis in respect of competent administrative authorities ordering online platforms to act against traders unlawfully promoting or offering products or services in the Union.**



## 5. WHAT IS LEGAL OFFLINE SHALL STAY UP ONLINE

Intermediaries should not be required to remove information that was legally published in the country in which they are established (their country of origin). The effect of removal orders issued outside the country in which the provider is established should be limited to the territory of the issuing Member State. This protects freedom of speech and media content, avoids conflicts of laws, avoids unjustified and ineffective geoblocking and ensures a harmonised digital single market. To avoid differing interpretations within the EU and respect free speech legislation outside the EU, this should also apply to violations of Union law. Nonetheless, it is of utmost importance to ensure that mechanisms are in place to deal effectively with illegal content. It is therefore problematic that the wording proposed by IMCO (Amendment 150) fails to ensure that the country in which the provider is established (country of origin) has the power to have illegal content removed in all cases without territorial limitation. Due to the limited effects on freedom of expression it is acceptable to allow for cross-border orders when it comes to commercial offers.

**Use case:** Meta/Facebook Ireland is blocking German users from accessing content which violates local laws on the “defamation of religions”. This can affect Muhammad cartoons and satire, for example. The DSA would allow German authorities to order the removal of such content even with effect for countries where they have been legally published.



### PAST EP RESOLUTIONS:

#### [EP Resolution 2020/2022\(INI\)](#), par. 15:

*"Underlines that a specific piece of content may be deemed illegal in one Member State but is covered by the right to freedom of expression in another; highlights that in order to protect freedom of speech, to avoid conflicts of laws, to avert unjustified and ineffective geo-blocking and to aim for a harmonised digital single market, hosting service providers should not be required to remove or disable access to information that is legal in the Member State that they are established in, or where their*

*designated legal representative resides or is established; recalls that national authorities can only enforce removal orders by independent competent authorities addressed to service providers established in their territory; considers it necessary to strengthen the mechanisms of cooperation between the Member States with the support of the Commission and relevant Union agencies;"*



### PLENARY AMENDMENTS PROPOSED BY LIBE:

#### [PLENARY AMENDMENT 518](#)

##### Recital 31

**+** Providers of intermediary services should not be legally required to remove content which is legal in their country of establishment. Competent authorities should be able to order the blocking of content published outside the Union only for the territory of the Member State where those competent authorities are established. This should be without prejudice to the right of providers to assess the compliance of specific content with their terms and conditions and subsequently remove non-compliant content even if it is not unlawful in their country of establishment.

#### [PLENARY AMENDMENT 527](#)

##### Article 8 - paragraph 2 - point b

the territorial scope of **+** an order addressed to a provider that has its main establishment in the Member State issuing the order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, does not exceed what is strictly necessary to achieve its objective;

### **PLENARY AMENDMENT 528**

Article 8 – paragraph 2 – point b a (new)

**+** the territorial scope of an order addressed to a provider that has its main establishment in another Member State is limited to the territory of the Member State issuing the order;

### **PLENARY AMENDMENT 529**

Article 8 – paragraph 2 – point b b (new)

**+** the territorial scope of an order addressed to a provider or its representative that has its main establishment outside the Union is limited to the territory of the Member State issuing the order;

### **PLENARY AMENDMENT 530**

Article 8 – paragraph 2 – subparagraph 1 a (new)

**+** First subparagraph, points (ba) and (bb), shall not apply where online platforms are ordered to act against traders established in the same Member State as the issuing authority, that are unlawfully promoting or offering products or services in the Union.



## 6. ENSURING THE FREE EXCHANGE OF LAWFUL INFORMATION AND MEDIA CONTENT ONLINE

Terms and conditions shall respect fundamental rights and permit interferences with the **free exchange of lawful information** only where it is incompatible with the declared purpose of the service. In order to give practical effect to the fundamental right to freedom of expression and media freedom, providers shall not be allowed to arbitrarily suppress legal content or act against those sharing it (e.g. by "de-platforming" them). The free exchange of opinions and information is essential to our society. Acting against legal content can be justified where content is incompatible with the declared purpose of the service.

**Use case:** The terms and conditions of some Internet providers ban posts on terrorism even if they criticise terrorist attacks (counter-terrorism) or if they constitute neutral media reporting.



### PAST EP RESOLUTIONS:

#### [EP Resolution 2020/2019\(INL\)](#), par. 34:

*"Underlines that the fairness and compliance with fundamental rights standards of terms and conditions imposed by intermediaries on the users of their services must be subject to judicial review; stresses, that terms and conditions unduly restricting users' fundamental rights, such as the right to privacy and to freedom of expression, should not be binding;"*



### PLENARY AMENDMENTS PROPOSED BY LIBE:

#### [PLENARY AMENDMENT 537](#)

Article 12 - paragraph 2 a (new)

**+** The terms and conditions of providers of intermediary services may exclude the hosting of lawful information from those services or otherwise limit the access to information that is lawful or suspend or terminate the provision of the service to recipients for providing lawful information only where the information is incompatible with the declared purpose of the service.

#### [PLENARY AMENDMENT 538](#)

Article 12 - paragraph 2 b (new)

**+** Terms and conditions of providers of intermediary services shall respect the essential principles of fundamental rights enshrined in the Charter.

#### [PLENARY AMENDMENT 539](#)

Article 12 - paragraph 2 c (new)

**+** Terms that do not comply with this Article shall not be binding on recipients.





## 7. BRINGING UPLOAD FILTERS IN LINE WITH FREE SPEECH AND MEDIA FREEDOM

Automated tools for content moderation and ex-ante content filters should only exceptionally be used by online platforms for ex-ante control to temporarily block manifestly illegal and context-insensitive content. Algorithms cannot reliably identify illegal content and routinely cause the suppression of legal content, including media content.

**Use case:** In 2021 Meta/Facebook filters prevented a German public broadcaster (WDR) from sharing an investigative broadcast on a terrorist attack in Hanau and mistakes made by the police. Five days later the company apologised for the “mistake” and made the video available, but the political debate on the findings was over by that time.



### PAST EP RESOLUTIONS:

#### [EP Resolution 2020/2019\(INL\)](#), par. 12:

"considers that mechanisms voluntarily employed by platforms must not lead to ex-ante control measures based on automated tools or upload-filtering of content..."

#### [EP Resolution 2020/2022\(INI\)](#), par. 12:

"Acknowledges the fact that, while the illegal nature of certain types of content can be easily established, the decision is more difficult for other types of content as it

requires contextualisation; warns that current automated tools are not capable of critical analysis and of adequately grasping the importance of context for specific pieces of content, which could lead to unnecessary takedowns and harm the freedom of expression and the access to diverse information, including on political views, thus resulting in censorship; highlights that human review of automated reports by service providers or their contractors does fully not solve this problem, especially if it is outsourced to private staff that lack sufficient independence, qualification and accountability;"



### PLENARY AMENDMENTS PROPOSED BY LIBE:

#### [PLENARY AMENDMENT 549](#) – TO MERGE WITH IMCO AM 21

##### Recital 25

+ Automated tools are currently unable to differentiate illegal content from content that is legal in a given context and therefore routinely result in over blocking legal content. Human review of automated reports by service providers or their contractors does not fully solve this problem, especially if it is outsourced to staff of private contractors that lack sufficient independence, qualification and accountability. Ex-ante control measures based on automated tools or upload filtering of content should exceptionally be permitted if the automated decision is reliably limited to information previously classified as manifestly illegal, irrespective of its context, the identity and the intention of the recipient providing it. Filtering automated content submissions such as spam should be permitted.

#### [PLENARY AMENDMENT 540](#) – TO MERGE WITH IMCO AM 138

##### Article 6

+ Providers of hosting services shall not use ex-ante control measures based on automated tools or upload-filtering of information for content moderation, except where

+ (a) automated content moderation decisions to remove or disable access to, or restrict proposals by recommender systems of, specific items are limited to information which is identical to information previously classified by qualified staff or a judicial authority as manifestly illegal<sup>4</sup> irrespective of its context, the identity and the intention of the recipient providing it, or has most likely been uploaded by automated means<sup>5</sup>;

+ (b) the technology used is sufficiently reliable to limit to the maximum extent possible the rate of errors where information is wrongly classified as illegal content; and

+ (c) the technology used does not prevent the accessibility and proposals by recommender systems of information which is not illegal content.<sup>6</sup>

4 According to the [Advocate General](#) providers should "...block only content which is 'identical' and 'equivalent' to that subject matter, that is to say, content the unlawfulness of which seems manifest ... In such cases, since an infringement is highly probable, that content may be

presumed to be illegal. It is therefore proportionate to block it preventively..."

5 To allow filtering of automated content submissions such as spam.

6 Safeguard in Art. 17 (7) of the Copyright Directive [2019/790/EU](#).

## 8. MY TIMELINE, MY CHOICE

The algorithm-driven spreading of problematic content should be contained by **giving users control over the algorithms prioritising the information that is presented to them** (recommender systems). Recording a person's behaviour online to personalise their timeline and recommendations should require their explicit consent. Additionally users should have the right to disable the platforms' controversial timeline algorithms and see their timelines in chronological order.

**Use case:** Documents leaked by Meta/Facebook whistleblower Francis Haugen found that the company's recommender algorithms negatively affect the mental health of teen girls, make the platform addictive to many users, and promote misinformation, toxicity, and violent content.

### PAST EP RESOLUTIONS:

#### [EP Resolution 2020/2018\(INL\)](#), recital X:

*"whereas the DSA should offer the possibility to opt-out, limit or personalise the use of any automated personalisation features especially in view of rankings and more specifically, offer the possibility to see content in a non-curated order, give more control to users on the way content is ranked;"*


#### [EP Resolution 2020/2019\(INL\)](#), Annex, recital (8):

*"In order to ensure, inter alia, that users can assert their rights, they should be given an appropriate degree of transparency and influence over the curation of content made visible to them, including the possibility to opt out of any content curation other than chronological order altogether. In particular, users should not be subject to curation without freely given, specific, informed and unambiguous prior consent. ..."*

### PLENARY AMENDMENTS PROPOSED BY LIBE:


#### [PLENARY AMENDMENT 521](#) – TO MERGE WITH IMCO AMENDMENT 290

Article 24a

 (new) Online platforms may process personal data concerning the use of the service by a recipient for the sole purpose of operating a recommender system only where the recipient has given his or her explicit consent as defined in Article 4, point (11), of Regulation (EU) 2016/679.

#### [PLENARY AMENDMENT 541](#)

Article 29 – paragraph 2 a (new)

 Very large online platforms that use recommender systems shall allow the recipient of the service to have information presented to them in chronological order only.