Council of the European Union

Brussels, 24 October 2025
(OR. en)

14280/25

Interinstitutional Files:
2023/0209 (COD)
2023/0210 (COD)

LIMITE

EF 350
ECOFIN 1376
CODEC 1586
ECB

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Payment Services: Technical Note from Commission Services on the digital Services Act and financial scams and the European Electronic Communications Code and the interplay with other legal acts in relation to fraud

[…]

REDACTED DOCUMENT ACCESSIBLE TO THE PUBLIC (20.01.2026). ONLY MARGINAL PERSONAL DATA HAVE BEEN REDACTED.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Platforms Policy and Enforcement
Coordination and Regulatory Compliance

Brussels
[redacted]

TECHNICAL NOTE FROM COMMISSION SERVICES

Subject: The Digital Services Act and financial scams; The European Electronic Communications Code and the interplay with other legal acts in relation to fraud

This document has not been adopted or endorsed by the European Commission and may not in any circumstances be regarded as stating an official position of the Commission. It is intended solely for information purposes to support the discussions between co-legislators in the negotiations process."

This technical note is provided to support co-legislators during technical discussions. The goal of this note is to describe, on the one hand, the scope of the Digital Services Act in the context of the fight against financial scams and actions undertaken in its enforcement. On the other hand, to clarify the definition of electronic communications services providers (ECSPs) pursuant to the European Electronic Communications Code and the interplay of the latter with other legal acts in relation to fraud.

The Digital Services Act in a nutshell

The DSA[1] aims to contribute to the proper functioning of the internal market, while also ensuring a safe, predictable, and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter are effectively protected. The DSA fully harmonises the obligations imposed, among others, on providers of intermediary services, including online platforms and online search engines, therefore pre-empting national rules in this area.

The DSA is horizontal and cross-sectorial legislation, as it **aims to tackle the dissemination of illegal content** that is not in compliance with Union law or the law of any Member State which is in compliance with EU law, irrespective of the precise subject matter or nature of that law. The DSA is neutral in that it does not define what constitutes illegal content: this is done in the applicable Union or national law. As a consequence, to the extent that practices such as online

[1] 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).

1

platforms, the providers of such services shall not be liable for the information stored, on condition that the said provider:

- does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or
- upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

The Court has already established in a rich case-law the application of these categories to a great variety of services. For example, Internet Service Providers, Wi-Fi hotspots or Domain Name System registrars can be considered mere conduits, whereas cloud services, such as Uploaded, and online platforms, such as eBay, Facebook or YouTube, are considered hosting service providers.

Article 6 DSA establishes a "knowledge standard", that refers to specific illegal content or activities. As clarified by Recital 22 DSA, the required actual knowledge or awareness "*cannot be considered to be obtained solely on the ground that that provider is aware, in a general sense, of the fact that its service is also used to store illegal content. Furthermore, the fact that the provider automatically indexes information uploaded to its service, that it has a search function or that it recommends information on the basis of the profiles or preferences of the recipients of the service is not a sufficient ground for considering that provider to have 'specific' knowledge of illegal activities carried out on that platform or of illegal content stored on it*".

Additionally, that Recital clarifies that "*[t]he provider can obtain such actual knowledge or awareness of the illegal nature of the content, through notices submitted to it by individuals or entities in accordance with this Regulation in so far as such notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content*". In this regard, Article 16 DSA requires providers of hosting services, including online platforms, to put in place mechanisms to allow individuals or entities to notify such providers of the presence of items of information that the recipients consider to be illegal content. According to Article 16(1) DSA, such notices are considered to give rise to actual knowledge or awareness of the relevant provider, for the purposes of meeting the "knowledge standard" described above.

In addition, after receiving the notice, Article 16 DSA obliges providers to process it in a timely and diligent manner and inform the user of the decision taken without undue delay and provide information on redress possibilities in respect of that decision.

The DSA merely harmonises the *exemption* of liability, i.e. the conditions under which providers of intermediary services shall not be held liable for the third-party content transmitted or hosted through its services. Where the exemption does not apply because the conditions are not met, the provider's liability claim can be processed under Union law or national, civil, commercial or criminal law. For instance, financial scams may be considered a fraud, and in many Member States, they are treated as a criminal offence. The attribution of liability will necessarily depend on the facts and circumstances of each case.

spoofing, phishing or impersonation (by means of deep fakes for instance) leading to **financial fraud** are **defined as illegal in EU or national law in compliance with EU law, the DSA applies** with respect to online platforms' and other online intermediary service providers' obligations regarding such illegal content.

1) Who is covered by the Digital Services Act?

The DSA applies to intermediary services offered to recipients of the service located in the Union and follows an asymmetric regulatory burden according to the Internet architecture, depending on their technical functionalities and on their size: intermediary services building the Internet or communication infrastructure (i.e. mere conduits and caching services) are subject to a light-touch due diligence regime, while hosting services are subject to additional obligations given their "user-facing" nature. Furthermore, hosting services that fall within the definition of online platforms are also subject to additional reinforced obligations and, lastly, the DSA imposes the most stringent level of due diligence obligations to the providers of online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million that have been designated very large online platforms (VLOPs) or very large online search engines (VLOSEs) by the Commission. The Commission has so far designated 25 VLOPs and VLOSEs, including Google Search, Facebook, Instagram, Tiktok or X.

Electronic communications service providers may fall within the definition of "mere conduit" under the DSA and may also fall under the scope of the Electronic Communications Code.

2) The liability regime of providers of intermediary services

Chapter II of the DSA ("liability") **harmonises the exemption of liability** of three kinds of services: mere conduits, caching and hosting services. In this particular context, the following two type of services are relevant:

- **mere conduit services**: according to Article 4 DSA, where the service is the transmission of information in a communication network, or the provision of access to a communication network, such as internet service providers, or interpersonal communication services, such providers shall not be liable for the information transmitted or accessed, on condition that the provider:
    - does **not initiate** the transmission;
    - does not **select the receiver** of the transmission; and
    - does not **select or modify the information** contained in the transmission.
- **hosting services**: according to Article 6 DSA, where the service consists of storage of information at the request of the recipient of the service, such as webhosting or online

faster takedown of scam content, including ads, and allowing the possible "actual knowledge/awareness" standard of the service provider is accelerated.

Finally, a voluntary **Code of conduct** (Article 45) dedicated to financial scams could be drawn up by relevant stakeholders, including the VLOPs and VLOSEs concerned to contribute to the proper application of the DSA in relation to risks linked to financial scams, allowing the signatory providers of VLOPs and VLOSE to take up tailored-made commitments relating to specific concerns, practices or risks leading to financial scams (e.g. certain advertising practices). The drawing up of a Code of conduct could involve ad intermediaries (e.g. demand-side platforms). Moreover, providers of VLOPs and VLOSEs who enter into a voluntary Code of conduct referred to in Article 45 DSA are required to subject themselves to an annual specific external audit to assess compliance with any commitments undertaken under such Code. As part of the DSA co-regulatory framework, once the Commission has assessed positively a Code of conduct under Article 45(3) of the DSA, it becomes embedded into the general DSA enforcement system. Indeed, adherence to and compliance with the commitments forming part of such a Code by a provider of a VLOP or VLOSE may be considered as appropriate risk mitigation measure under Article 35 of the DSA. Therefore, as part of the DSA co-regulatory framework, such a Code of conduct may become a significant and meaningful benchmark for determining compliance with DSA obligations and the lack of compliance by the signatory providers with the commitments undertaken in such a Code may entail reputational and financial consequences for the providers of VLOPs and VLOSEs concerned.

4) Enforcement of the DSA

The DSA lays down a system of shared competences for the enforcement and supervision of compliance with the DSA.

While the Commission has exclusive powers to supervise, monitor and enforce Section 5 of Chapter III of the DSA (i.e. the most stringent due diligence obligations) in respect of providers of VLOPs and of VLOSEs' compliance with the DSA , the Member State where the main establishment of the provider of intermediary services is located has, pursuant to Article 56(1) DSA, exclusive powers to supervise and enforce all the other the obligations of that Regulation that apply to the concerned provider, including, vis-à-vis providers of VLOPs and VLOSEs, in so far as the Commission has not initiated proceedings for the same infringements.

On 30 April 2024, the Commission adopted a decision initiating proceedings against the providers of **Facebook** and **Instagram** to assess whether **those providers** may have breached the DSA. The suspected infringements cover**, among other areas, Meta's policies and practices relating to deceptive advertising and coordinated inauthentic behaviour for the dissemination of financial scams in the EU. In addition, the Commission issued requests for information on 23 September 2025 to Apple App store, Booking.com, Bing, Google Play and Google Search on how these platforms and search engines identify and manage risks related to financial scams.**

In parallel, several providers of **VLOPs and VLOSEs —such as LinkedIn, Pinterest, Google Play, YouTube, Temu, and XNXX**— have begun to acknowledge financial scam risks in their annual risk assessments which they are obliged to carry at least once per year and whenever they deploying new functionalities that are likely to have a critical impact on the risks which they are obliged to manage under the DSA.

The Commission recognises the **growing concern from the payments and banking sectors** regarding the role of platforms in online fraud, and is prioritising enforcement in this area, together with the Digital Services Coordinators at national level. The issue was formally raised at the **European Board for Digital Services** on 29 April 2025 and further discussed during **Working Group 5 (Online Marketplaces)** on 16 June, where the Commission launched a **dedicated workstream on financial scams**. A **deep dive on financial scams** was also held during the Digital Services Board meeting on 27 June 2025 and 23 September 2025, marking a key step in aligning EU and national enforcement responses.

More information:

- Digital Services Act – policy page
- Digital Services Act – Q&A Memo
- Digital Services Act – fact page
- The enforcement framework under the Digital Services Act
- The cooperation framework under the Digital Services Act
- Supervision of the designated very large online platforms & search engines under DSA
- Trusted flaggers under the Digital Services Act (DSA)

The European Electronic Communications Code (EECC) and the interplay with other legal acts in relation to fraud

1) Definitions of relevant services

The **European Electronic Communications Code (EECC)** provides the relevant definitions that are needed to identify the different categories of electronic communications services providers (ECSPs) and to understand which ones could fall within the scope of the PSR.

According to article 2 (4) EECC, **'electronic communications service'** (ECS) means a service which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

a) **'internet access service'** (IAS), which - as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120 **(Open Internet Regulation)** - means a publicly available **electronic communications service** that provides access to the internet, and thereby

connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used;

b) **interpersonal communications service (ICS);** and

c) **services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;**

With regard to point b), Article 2 (5) defines an ICS as a service normally provided for remuneration, but not necessarily linked to monetary value (Recital 16 EECC) : that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

There are two categories of ICS:

- **'number-based interpersonal communications service' (NB-ICS)** means an ICS which connects with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which enables communication with a number or numbers in national or international numbering plans. This corresponds, for instance to SMS, Rich Communication Services (RCS) and number-based calls, and is a service typically provided by mobile and fixed electronic communications providers, although recently number-independent interpersonal communication services started to provide access to numbers in the national or international numbering plan (Teams, WhatsApp);

- **number-independent interpersonal communications service' (NI-ICS)** means an ICS which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans. This corresponds, for instance, to services such as e-mails, Signal, Viber (ViberIn/Viberout), WhatsApp, Microsoft Teams (which does also offer access to numbers in the national or international numbering plan while the main service is provided between two accounts, as opposed to two numbers).

Therefore, services such as **voice telephony** (both traditional and Voice over IP)**, messaging services** (SMS, RCS and number-independent ones) **and electronic mail services** (including web-based) **fall within the scope of ECS and are covered by the EECC**. Certain ECS may also be covered by the Directive (EU) 2015/1535 (the Information Society Service Directive) to the extent that the EECC (Recital 10 EECC) and respectively, the DSA or other Union acts, do not contain more specific provisions applicable to ECS. It has to be noted that the same undertaking, for example an **internet service provider, can offer both an electronic communications service, such as access to the internet, and services not covered by the EECC, such as the provision of web-based and not communications-related content** -

7

As a result, rather than focusing on the providers, it is advisable to focus on the services that are relevant for the purpose of the PSR, which are ICS.

2) Fraud-related measures in the EECC

The EECC does neither provide a definition of fraud, nor concrete technical solutions to ensure the prevention of fraud.

Article 97 (2) provides that Member States should ensure that national regulatory authorities or other **competent authorities are able to require relevant ECSPs to block, on a case-by-case basis, access to numbers or services (under Article 97(1): use services using non-geographic numbers within the Union) where this is justified by reasons of fraud or misuse** and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues.

This provision was introduced in the electronic communications framework preceding the 2018 EECC by the Citizen's Rights Directive in 2009 and it was not changed in the EECC. Therefore, the scope of the article was limited to number-based services (also because it was/is part of the numbering section).

Recital 254 seems to envisage cases of caller ID spoofing where international tariffs are fraudulently charged from the victims and fraudulent activities consisting of bypassing interconnection tariffs. As for the services referred to in Article 97(2), the recital explains that they are those that 'use services using non-geographic numbers within the Union', hence it may be inferred that Article 97(2) is limited in scope to enabling Member States to require operators to block numbers and such number-based services.

The teleological interpretation of Article 97(2) may lead to the conclusion that **the legislator focused on fraud schemes linked to the avoidance of higher termination tariffs where the victims are the terminating operators and, possibly, end-users that are not aware of the actual termination rates when lured into calling a number**.

It is worth noting that **such a measure would not intrude into the content of the communication, but it would be taken on the basis of the number from which the communication is originated (metadata).**

While the scope of the publicly available electronic communication services was clarified in the EECC to include both, number based and number independent ICS, **the article was not designed in 2009 to prevent impersonation fraud** perpetrated via both number base and number independent ICS as the main measure proposed is blocking the number or a service accessible via a number.

However, such provision offers a potential solution for cases of impersonation fraud happening via NB-ICS. Competent authorities may accordingly require providers of NB-ICS to block access to numbers or services used to commit impersonation fraud. With the required differences, the same could be envisaged also for NI-ICS.

Looking at preventive measures, while concrete technical solutions are not mandated, Article 103 (4) provides that internet access providers and publicly available number-based interpersonal communication services distribute **public interest information free of charge to existing and new end-users,** by the means that they ordinarily use in their communications with end-users. Such information should include a) **the most common uses of internet access services and publicly available NB-ICS to engage in unlawful activities or to disseminate harmful content,** and b) **the means of protection against risks to personal security, privacy and personal data** when using internet access services and publicly available number-based interpersonal communications services.

3) **Preventive measures in the Network and Information Security (NIS2) Directive (Directive (EU) 2022/2555)**

The NIS2 Directive impose **obligations on ECSPs to undertake measures to ensure the security of network and information systems** as well as to prevent or minimize the impact of incidents on recipients of their services and on other services.

According to Article 6(1) of the NIS2 Directive, **network and information systems** include a) electronic communications networks, b) devices carrying out automatic processing of digital data, c) **digital data stored processed, retrieved or transmitted** by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

According to Article 6 (2) of the NIS2 Directive, **security** of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any **event that may compromise** the availability, **authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems.**

In terms of the measures the ECSPs are required to implement the following:

a) **policies on risk analysis and information system security**;
b) **incident handling**, whereby **incident** is an event compromising the availability, **authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems**;
c) business continuity, such as backup management and disaster recovery, and crisis management;
d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
g) **basic cyber hygiene practices and cybersecurity training;**
h) **policies and procedures regarding the use of cryptography and, where appropriate, encryption**;

i) **human resources security, access control policies and asset management;**
j) **the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications** and secured emergency communication systems within the entity, where appropriate.

Therefore, whenever an event could compromise the authenticity, integrity or confidentiality of the services offered, (e.g. involving **an interference with the service provided by the ECSPs** etc.), it could qualify as a "cyber incident", which, if significant, is subject to reporting to the competent authorities as required by Article 23 of the NIS 2 Directive. (More details: *ENISA Threat Landscape: Finance Sector, Report for the period January 2023 to June 2024*). That is why, the ECSPs have obligations to undertake the above measures.

4) Obligations concerning the privacy of electronic communications: the ePrivacy Directive (Directive 2002/58/EC/ePD)

The ePD ensures an equivalent level of protection of the right to privacy and confidentiality with respect to the processing of personal data in electronic communications, and provides limited exceptions to it.

Article 5(1) obliges Member States to have in place **national legislation to ensure the confidentiality of communications and the related traffic data** by means of a public communications network and publicly available electronic communications services. In particular, **such legislation shall "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned**".

Thus, according to Article 5(1), not only the content of interpersonal communications (including the content of emails and SMS), but also the related traffic data is protected under the confidentiality obligation. Such data can only be processed either with the consent of the user or, exceptionally, when it is technically necessary for the conveyance of the communication.

Article 6 lays down the **situations where the traffic data can be processed by the provider of a publicly available electronic communications services**, in particular, for the purpose of the transmission of a communication (i.e. **for billing and interconnection payments**, for **marketing of electronic communications services** or providing **value added services**).

Furthermore, Article 15(1) foresees the possibility for Member States to adopt legislative measures restricting obligations under Articles 5 and 6 when necessary "to safeguard national security (i.e. State security), defence, public security, and the **prevention, investigation, detection and prosecution of criminal offences** or of **unauthorised use of the electronic communication system".**

Other provisions that are relevant concern the treatment of **calling and connected line identification (CLI)**, that is to say when the calling party's number is presented to the called

party prior to the call being established. This is relevant also for those ECS provided over IP. CLI **is needed for tracing nuisance, and malicious communications which could be fraudulent as well**.

Article 8 concerns the **mechanisms for user identification and privacy control**. The ECSP must offer the calling user the possibility, using a simple means and free of charge, of **preventing the presentation of the calling line identification on a per-call basis**. The calling subscriber must have this possibility on a per-line basis. The ECSP should also give the **possibility to the called subscriber to reject incoming calls where the presentation of the CLI has been prevented by the calling user or subscriber**.

Article 10 provides, for certain limited purposes, exceptions **to the rights for presentation and restriction of calling and connected line identification** and allows Member States to override these rights **in the case of emergency calls or while tracing malicious or nuisance calls**. The elimination of the presentation of CLI is possible **on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls.** In this case, **in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network** and/or publicly available electronic communications service.

This article is **relevant for fighting fraudulent calls**.

5) Open Internet Regulation (OIR, Regulation (EU) 2015/2120)

The OIR is a crucial instrument, which grants end-users the directly applicable right to access and distribute lawful content and services of their choice via their Internet access service but also enshrines the principle of non-discriminatory traffic management. Reasonable traffic management is possible, only when necessary and for as long as necessary, in restricted circumstances.

More precisely, Article 3 states that **providers cannot** implement traffic management measures that **block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, except when it is necessary and only for as long as necessary** a) **to comply with EU or national legislation or court orders**, b) **to preserve the integrity or security of the networks, the services using the networks, or the end-user equipment**, or c) to prevent an impending network congestion, which is temporary and exceptional.

Points a) and b) could offer a potential legal basis for initiatives intended to stop ex post (a) and prevent (b) fraud.

6) **Treatment of personal data**

When looking at preventive measures, account must be taken of the need for ECSPs to preserve the confidentiality of communications and to process personal data in accordance with the GDPR. In October 2024, the European Data Protection Board issued Guidelines covering the processing of data for the purposes of fraud prevention, network and information security, for which processing relies on legitimate interests.

In any event, ECSPs are prevented from general monitoring the content of communications.

7) **Examples of anti-fraud measures adopted by Member States for ECS providers:**

Therefore, the abovementioned legal instruments provide room for prevention through technical measures.

Member States have been empowered to adopt measures at national level, which so far have focused on services provided by NB-ICS. 11 EU Member States have already adopted anti-spoofing measures and others are in the process of adoption, as follows:

a) Measures for blocking incoming international calls:
Operators block calls originating from abroad and using a national number as CLI.

Blocking of fixed numbers is more widespread.

Some national measures also require blocking mobile numbers, while addressing the issue of legitimate roaming users.

b) Do-not-originate registry
National database of numbers that can never be used for outgoing calls.

Examples include numbers of banking services, premium numbers, emergency numbers, numbers for directory services.

c) Protected numbers registry
List of phone numbers that the NRA did not assign, and which cannot be used to originate calls.

Examples include calls when the CLI field is empty, not assigned to any service or not consistent with the national numbering plan.

d) SMS Sender ID Registry
Registry of alphanumeric SMS sender ID.

Operators must block SMS with a sender ID that is not registered, or when the sender is not the registered source.

e) STIR/SHAKEN

STIR/SHAKEN requires providers to authenticate and digitally sign the caller's ID at the call origination and verify it at the termination.

Works on all-IP networks (not on legacy Public Switched Telephone Networks).

f) Action against unreliable websites

This solution allows for setting up blacklists by the Cybersecurity Centres according to which the ISPs could check on its DNS server if the website is reliable and prevent access to it if fraudulent (the measure does not include shutting down the website).

It is important to mention that spoofing of numbers concerns NB-ICS and not NI-ICS, but authentication measures are possible for NI-ICS too and should be applied with preventive purposes i.e., obligations to authenticate the user to avoid NI-ICS scams.

It is worth mentioning that most of the national measures have been adopted quite recently (since 2024), hence it is premature to have a clear view of their effects in practice. Furthermore, being overly prescriptive towards the ECSPs runs the risk that the measures would shortly become outdated, given the pace of evolution of fraud and at the same time, not providing a workable solution against the perpetrators. On the contrary, obliging, for instance, ECSPs to reimburse victims of fraud is an additional incentive for malicious actors.