FEDOWEB

FEDERAZIONE OPERATORI WEB

Milan, January 18, 2024

This contribution to the public consultation, promoted by the European Data Protection Board (***EDPB***), on the draft "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive" (***Guidelines***) is filed by Fedoweb.

Fedoweb - the Federation of web operators (*Federazione Operatori Web*) was created in 2000 to meet the requirements of the on-line market and promote the internet as a means of advertising and communication. Today, Fedoweb brings together the main publishing groups and television broadcasters and the leading web operators and stands out in the Italian market owing to the different media it represents. The main areas in which Fedoweb works relate to changes to business and regulators which the digital revolution has brought about in advertising, communications and media. Privacy, digital platforms for advertising and content distribution, the audience survey metrics, as well as standard rules for all web operators, are some of the issues that Fedoweb continuously monitors. Among other things, Fedoweb is a quotaholder of Audicom Srl, which is the Joint Industry Committee (***JIC***) that measures, for Italy, the audience of multimedia, editorial and/or advertising content through both the Internet and paper press.

Fedoweb's members include: 3BMeteo, Ansa, Ciaopeople, Classeditori, Condé Nast, Gedi Gruppo Editoriale, Il Fatto quotidiano, Il messaggero, Il Sole 24 Ore, Italiaonline, Mondadori, Rai, RCS, RTI Interactive Media, Speed.

This contribution is made without prejudice to the position and/or contribution that may be taken independently by Fedoweb's members, which are therefore free to propose additional views.

In light of the purpose of the Guidelines ("*The aim of these Guidelines is to conduct a technical analysis on the scope of application of Article 5(3) ePD, namely to clarify what is covered by the phrase 'to store information or to gain access to information stored in the terminal equipment of a subscriber or user'. These Guidelines do not intend to address the circumstances under which a processing operation may fall within the exemptions from the consent requirement provided for by the ePD*"), this contribution is focused on Article 5(3) of Directive 2002/58/EC (***ePD***) and aims at **reminding** the EDPB of:

a. the acknowledged ineffectiveness of Article 5(3) ePD and of its consent requirement in protecting data subjects' rights and interests, which led to the proposal of a "Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and **repealing Directive 2002/58/EC** (Regulation on Privacy and Electronic Communications)" (***ePrivacy Regulation***);
b. the risks of a broad interpretation of the scope of application of Article 5(3) ePD, specifically for the news media sector;
c. the importance of, and need for, creating new specific exceptions to the consent requirement, to allow for the processing of data that causes little to no impact on the rights of the secrecy of communications and private life.

All the above issues have already been acknowledged by both the European Institutions and by the Article 29 Data Protection Working Party (***WP29***, i.e. the predecessor of the EPBD), which recognized (i) on the one hand, that Article 5(3) ePD causes an unnecessarily high burden for businesses not counter-balanced by an

equally high usefulness for data subjects, and (ii) on the other hand, the need to identify more exceptions to the consent requirements under Article 5(3) ePD also in light of the importance of ensuring the EU goal of establishing a Digital Single Market and of promoting data-driven innovation.

As widely known, said issues and needs were supposed to be addressed during the revision of the ePD through the implementation of the ePrivacy Regulation and, indeed, the ePrivacy Regulation - and, in particular, its latest available draft dated 10th February 2021 - proposed to modernize Article 5(3) also by including more exceptions to the consent requirement provided by the ePD. However, the institutional negotiations on the ePrivacy Regulation took (much) longer than expected, and European Institutions were recently reported to have decided to suspend works on the ePrivacy Regulation and to address the same issues and needs during the forthcoming review of Regulation (EU) 2016/679 (***GDPR***)[1].

In a context where the consent requirement of Article 5(3) ePD proved to be ineffective and discussions to introduce more exceptions to the consent requirement where ongoing, the Guidelines came as a great surprise: their extensive interpretation of the scope of Article 5(3) ePD, together with the lack of cases where non privacy-intrusive tracking technologies can be used without the data subjects' prior consent, thus losing a great opportunity to contribute to a concrete protection to data subjects' rights by reducing the consent fatigue and – among others - by ensuring media pluralism and media quality.

In the below paragraphs, we will address the main reasons for narrowing the interpretation of Article 5(3) ePD and introducing more exceptions to the consent requirement.

***

A. The acknowledged ineffectiveness of Article 5(3) ePD in protecting data subjects' rights and interests and the reasons/circumstances for the proposal of the ePrivacy Regulation.

One of the key points of the European Commission's proposal for the ePrivacy Regulation (which, for the sake of completeness, should have substituted the ePD) was to **simplify rules on cookies**: "*the cookie provision, which has resulted in an overload of consent requests for internet users, will be streamlined. The new rule will be more user-friendly as browser settings will provide an easy way to accept or refuse tracking cookies and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies that improve internet experience, such as cookies to remember shopping-cart history or to count the number of website visitors*"[2].

Article 5(3) ePD has indeed proved to be **only partially effective** in protecting data subjects' rights and interests.

In particular, as highlighted in the final report "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector"[3]:

[1] See https://globaldatareview.com/article/official-commission-could-cut-its-losses-eprivacy-regulation?utm_source=Official%253A%2BCommission%2Bcould%2Bcut%2Blosses%2Bon%2BePrivacy%253B%2BJudge%2Blets%2Bsome%2Bsocial%2Bmedia%2Bproduct%2Bclaims%2Bcontinue&utm_medium=email&utm_campaign=GDR%2BAlerts .

[2] Ref. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation .

[3] The report is available at https://digital-strategy.ec.europa.eu/en/library/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector .

- "*Based on our findings, there is **room for improvement as concerns the effectiveness of this provision.** Although some strengths have been identified, several challenges were raised by various stakeholders and in the literature. These include in particular ambiguities in relation to the scope of this provision, the fact that the scope may be too broad, limited transparency and effectiveness of the consent mechanism as well as difficulties relating to enforcement. Based on these challenges, this provision is burdensome for businesses, while the effective added value for citizens may be improved*";
- "*[…] for some users and subscribers it may not be clear that giving mere consent can provide a justification to comprehensively track their behaviour in the online environment ("profiling"). On this basis, giving consent might trigger that users get a false sense of protection. Similarly, it was pointed out at the workshop the Commission held with competent authorities that there is a danger of an information overload and too much complexity*";
- "*For example, during the meeting the Commission held with competent authorities in 2016, participants pointed out that the varying enforcement in the Member States has resulted in an **unequal level playing field and market distortions**. Some Member States enforce the article focusing only on privacy-intrusive cookies (tracking cookies) instead of covering all relevant aspects according to the ePD. There is room for manoeuvre whether the use of cookies with low risk to threat privacy should depend on consent or whether they should rather be set by default. Based on these issues relating to the scope, the consent mechanism and enforcement, competent authorities interviewed by Deloitte pointed out that this provision causes an **unnecessarily high burden for businesses, while the usefulness for citizens is not optimal***";
- "*The efficiency of Article 5(3) is not fully ensured. This is due to the fact that this provision tends to be the main cost factor associated by businesses with the ePD, while not all the costs appear to be justified and the benefits for citizens have been questioned. In particular, based on the ambiguities relating to the scope and consent mechanism, businesses may spend more time than needed on implementing the consent mechanism and possibly need to invest in legal advice. Furthermore, based on the fact that Article 5(3) does not make a distinction between different types of cookies, businesses that only use non-privacy invasive cookies also need to obtain consent. At the same time, users feel annoyed by the consent mechanism, which often does not provide a real choice*";
- "*[…] the WP29 and other stakeholders consulted indicated that, while it is relevant to retain Article 5(3), the content is not fully appropriate in light of the market situation and technological development. This was based in particular on the fact that the article does not make a distinction between different types of cookies and that the usefulness for users is questioned (see section 5.7.1). This is, e.g. reflected in Deloitte's online survey with competent authorities. The majority of respondents (19 out 30, 63%) indicated that the provision is "important to retain, but with changes". In addition, two authorities indicated that is "important to retain as is" and two that it is "useful to retain, but with changes". No authority indicated that this provision does not need to be retained*";
- "*In addition, some stakeholders have argued that aspects of this provision are not in line with the goal of the EU to establish a **Digital Single Market.** More specifically, it was argued at a stakeholder workshop organised by the Commission that forbidding the tracking of users (and related techniques) could hamper data-driven innovation. This is confirmed by the fact that several interviewees from the business perspective indicated that the provision is quite burdensome for businesses that need to comply with it as well as the advertisement industry. However, this may be justified at least partially by the rationale to **protect the privacy of citizens,** which is fully in line with the general goal of the EU to protect the fundamental rights of its citizens*".

The results of the mentioned report confirmed the findings of the study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation"[4], where the European Commission had noted that "*It is difficult to deny that the introduction of the consent rule in Art. 5.3 has not entirely reached its objective. This is largely due to the fact that users currently receive a warning message with regard to the use of cookies on almost every web site. Obviously the effect of such warning messages would substantially increase if they only appeared where a web site contained 3rd party cookies, cookies used for direct marketing purposes and, more generally, all cookies that are not related to the purpose for which the user is navigating on the site. This is without prejudice of including appropriate warnings and consent mechanisms whenever someone wants to access any privacy sensitive information (pictures, emails, contact lists) that users may have in their terminal equipment, via any mechanisms other than cookies*".

Finally, also the explanatory memorandum to the ePrivacy Regulation highlighted that the ePD "*did not fully met its objectives. The unclear drafting of certain provisions and ambiguity in legal concepts have jeopardized harmonization, thereby creating challenges for businesses to operate cross-border. The evaluation further showed that some provisions have created unnecessary burden on businesses and consumers. For example, the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning and, in some cases, are even exposed to cookies being set without their consent. The consent rule is over-inclusive, as it also covers non-privacy intrusive practices, and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device. Finally, its implementation can be costly for businesses*"[5].

In light of such ascertained inefficiency of Article 5(3) ePD, there is clearly no usefulness in expanding its scope of application by extending the consent requirement and/or omitting the identification of specific exceptions to the same consent requirement.

Indeed, by doing so, **the Guidelines may further reduce the effectiveness of Article 5(3) ePD by – in particular - significantly increasing the so-called consent fatigue**.

The European Commission is currently trying to address the consent fatigue by promoting the "cookie pledge initiative", aimed at agreeing on voluntary practices "*to better empower consumers to make effective choices regarding tracking-based advertising models*"[6]. It is widely known that the consent fatigue led to consents being granted (or denied) very lightly, i.e. with no real reasoning and real comprehension by the users. Therefore the Guidelines, by extending the scope of Article 5(3) ePD and the consent requirements, not only are contrary to the European Commission's efforts and purposes, but also may end up reducing the protection for the data subjects as it is also ascertained that individuals are increasingly accepting and/or refusing to grant consent without real knowledge.

[4] This study is available at https://digital-strategy.ec.europa.eu/en/library/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data .
[5] See https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications .
[6] See https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en .

B. The risks of a broad interpretation of the scope of application of Article 5(3) ePD, specifically for the news media sector.

In its "Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)" adopted on 19 July 2016, the WP29 noted that "*There is a clear democratic need to ensure the economic survival of news media. However the EC should not accept that news media impose invasive tracking of users*".

This is a clear acknowledgement, by the WP29 (and, consequently, by the EDPB), of the consequences that a broad interpretation of the consent requirement under Article 5(3) ePD will have for the news media sector: a severe reduction of advertising investments, which will put the news media sector's survival at risk.

The costs of complying with Article 5(3) ePD have already been identified as **high** by the final report "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector"[7]:

- "*As part of the interviews carried out, business associations in the area of newspaper and online publishing (digital news and media content) have indicated that their members can be reasonably expected to incur up to 120,000 EUR of initial compliance costs to set up a cookie banner on their website and related technical changes. In addition, the total maintenance costs add 80,000 EUR to 130,000 EUR to this initial investment. Thus, according to this information, businesses in the publishing industry incur a total amount of between 200,000 EUR and 250,000 EUR (i.e. not per annum but over time) for the compliance of their websites with Art. 5(3). Such an estimate serves to balance the general applicability of the 900 EUR estimated by ITIF for website compliance towards specific types of businesses*";
- "*[…] some businesses do incur significant **compliance costs** in relation to this provision. It was, furthermore, pointed out by the businesses and business associations consulted as part of this study that **opportunity costs** occur. For the businesses complying with this provision and the advertisement industry, opportunity costs may, according to the interviewees, be based on the dissuasive effect on users, who may stop using the services of a websites. The fears of users may not always be legitimate, as also websites using non-privacy invasive cookies need to install a consent mechanism. Especially, small or medium sized businesses referred to the opportunity costs that they experienced due to the cookies provisions which threatens their business potentials. They experienced loss of revenue as they lose users and it is too costly for them to obtain consent. Based on the shortcomings identified in relation to the effectiveness of this provision (see section 5.7.1), **not all these costs appear to be justified.** Notably, based on the ambiguities relating to the scope and consent mechanism, businesses may spend more time than needed on implementing the consent mechanism and possibly need to invest in legal advice. Furthermore, based on the fact that Article 5(3) does not make a distinction between different types of cookies, businesses that only use non-privacy invasive cookies also need to obtain consent. Based on the 2014 Cookie Sweep, 74 out of 474 websites only used first party cookies. In addition, 15 out of 474 only used session cookies (first and third party). Turning to the **perspective of the user,** there may be a risk that users are overburdened with giving consent in situations where it is not absolutely necessary. This is closely related to the critique that the article does not contain sufficient exceptions. In addition, frequent consent mechanisms, such as banners on websites, might disrupt the users' Internet experience according to the advertising industry.*

[7] The report is available at https://digital-strategy.ec.europa.eu/en/library/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector .

Furthermore, it was pointed out in the previous sub-section that the effectiveness of the cookie banner is hindered, in particular because the consent mechanism may not be sufficiently transparent and users do not have a real choice as access to services is typically denied if they do not consent to cookies. As the benefits for users are limited, it can be argued that the high costs for businesses are not justified".

For a comprehensive assessment of the costs of complying with Article 5(3) ePD, also the losses in advertising investments shall be taken into account[8].

Should data controllers be required to collect the data subjects' consent for almost all trackers that do not fall in the strict exceptions to the consent rule, this would lead to the following consequences:

- the measurement of advertising effectiveness will be distorted by default. Users may not be inclined to provide their consent to processing (often for reasons other than a non-acceptance of the purpose of processing, attributable simply to the consent fatigue and the greater ease of withholding consent instead of investing time in reading and understanding the privacy notices) and fewer consents correspond to a lower volume of measured subjects and, therefore, to a (perceived) lower effectiveness of the advertising campaign being measured;
- advertising campaigns (perceived as) less effective mean less advertising investments;
- less advertising investments mean fewer resources for publishers;
- fewer resources for publishers mean greater survival risks for them;
- the risks of survival for publishers result in the reduction of voices in the market and, therefore, in the compression of the right to information, including in its meaning as the right to pluralism of information, but also in greater risks of misinformation and disinformation.

The above risks have been acknowledged also in the ePrivacy Regulation (e.g. in Recital 21 aa of the draft dated 10th February 2021[9]: "*In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment* ***may also be necessary for providing a service, requested by the end user, such as services provided in accordance with the freedom of expression and information including for journalistic purposes, e.g. online newspaper or other press publications as defined in Article 2 (4) of Directive (EU) 2019/790, that is wholly or mainly financed by advertising*** *provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar techniques and has accepted such use*")[10].

Misinformation and disinformation have been listed among the main short-term risks of 2024, by way of example, by the World Economic Forum[11].

C. The importance of, and need for, creating new specific exceptions to allow for the processing of data that causes little to no impact on the rights of the secrecy of communications and private life.

[8] By way of example only: the Italian Federation of Media Agencies (*Federazione Concessionarie Pubblicità*) estimated an economic loss for 2024 equal to 20% of the aggregate turnover of their members, if compared to 2023.
[9] Published at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf .
[10] Emphasis added.
[11] The Global Risks Report 2024 issued by the World Economic Forum is available at https://www.weforum.org/publications/global-risks-report-2024/ .

Both the European Institutions and the WP29 have already acknowledged the importance of, and the need for, a broad interpretation of the exceptions to the duty to obtain data subjects' prior consent under Article 5(3) ePD.

By way of example, in the study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation"[12], the European Commission considers that the rules on cookies and similar techniques may have not entirely achieved their objectives, given that users receive too many warning messages which they do not properly consider. Therefore, the study recommends maintaining the current opt-in approach to cookies, but **limiting it only to situations where there is an interference with users' privacy (including websites serving third party cookies for behavioural advertising purposes, excluding analytics cookies)**. This result may be achieved, for example, by broadening and/or clarifying the exceptions to the cookie consent rule (which allows the placing of cookies in the users' terminal equipment or equivalent web-tracking techniques only with the users' prior and informed consent).

In greater detail:

- "*Article 5.3 currently contains two exceptions where prior consent of the user is not needed: a) for the technical storage of, or the gaining access to information for the sole purpose of carrying out the transmission of a communication over an electronic communications network and b) for the provision of an information society service that is explicitly requested by the subscriber or the user, when the storing of or the gaining access to information is strictly necessary for the provider. These exceptions should preferably receive a slightly broader formulation, for example, by deleting the condition stating that "the storing of or the gaining access to information (should be) strictly necessary for the provider"*";
- "*Last but not least, while the current discussion mainly deals with the issue of how consent should be given and how the relevant information should be furnished to the user or the subscriber, it should also be examined whether the choice to make the ePrivacy Directive allow the use of cookies (and similar techniques) based only on the consent of the user or the subscriber is effective and logically plausible. Does the consent of the user justify unlimited tracking of that user's behaviour in the online environment, given the known weaknesses of consent as a mechanism for ensuring legitimacy? This question inevitably leads us to the issue of "profiling", and any solution should take into account the outcome of the discussion in the framework of the proposed general Data Protection Regulation on this very issue*".

Also the WP29, in its "Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)" adopted on 19 July 2016, recognized the need for more exceptions to the consent rule: "*while clarifying the broad scope of the consent requirement, the EC should also create more specific exceptions, to allow for the processing of data that causes little or no impact on the rights of users to secrecy of communications and private life*".

Such need is even more urgent, considering that the definition of "necessity" is being interpreted in an increasingly restrictive way in the data protection field.

[12] This study is available at https://digital-strategy.ec.europa.eu/en/library/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data .

Consent should be considered as non-necessary not only when the sole purpose of processing is carrying out the transmission of a communication over an electronic communications network, or when the tracker is necessary in order for the provider of an information society service to provide a service explicitly requested by the subscriber or user; there may indeed be cases where the tracker does not satisfy these requirements but is nevertheless not privacy-intrusive and does not carry out any risks for the data subjects, either for the purposes of processing or for the technical safeguards implemented.

This could be the case, e.g., of those trackers used for fraud prevention purposes, or for service improvement purposes: in such cases, not only the processing is not privacy-intrusive, but goes also to the benefit of the data subject. And it could also be the case of the trackers used for the sole purpose of audience measurement; besides, the personal data processed is pseudonymized in such a way that the data can be considered as almost anonymous.

With regards to audience measurement activities, it is important to remind that Fedoweb is a quotaholder of Audicom, and that Audicom cooperates with Auditel (Audicom and Auditel are both JICs) for integrated audience measurement activities in the Italian media sector. For the sake of completeness, **audience measurement** is "***the activity of collecting, interpreting or otherwise processing data about the number and characteristics of users of media services or users of content on online platforms*** *for the purposes of decisions regarding advertising allocation or pricing or […] planning, production or distribution of content*"[13] and it is carried out, by Audicom and Auditel, in the public interest[14].

Both Audicom and Auditel are subject to the regulatory oversight of the *Autorità per le Garanzie nelle Comunicazioni* or ***AGCOM***, i.e. the Italian Communications Authority. Indeed, AGCOM is empowered to "*ensure, also in light of the processes of multimedia convergence, that the measurement of audience and readership indices of the various media, on any distribution and broadcasting platform, conform to criteria of methodological correctness, transparency, verifiability, and certification by independent subjects, and are carried out by bodies endowed with the utmost representativeness of the entire reference sector. The Authority issues the necessary directives to ensure compliance with the above criteria and principles and supervises their implementation […]*"[15].

As noted in the "Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU": "***audience measurement has a direct impact on the allocation and the prices of advertising, which represents a key revenue source for the media sector****. It is a crucial tool to evaluate the*

[13] This is the definition of "audience measurement" provided by the latest version of the "Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU", available at https://www.consilium.europa.eu/en/press/press-releases/2023/06/21/european-media-freedom-act-council-secures-mandate-for-negotiations/ .

[14] This has been confirmed also, inter alia, in the "Yearly Report 2023" published by Auditel at https://www.auditel.it/wp-content/uploads/2023/03/Relazione-Annuale-Auditel-2023-def.pdf and forwarded to the Italian Parliament.

[15] Article 1, paragraph 6, letter b, point 11 of Italian Law 249/1997.

performance of media content and understand the preferences of audiences in order to plan the future production of content"[16].

Considering such direct impact of audience measurement on advertising investments, it is even more important to ensure that also audience measurement – in particular when carried out by entities, such as Audicom and Auditel, subject to a public authority's oversight and pursuing a public interest – are granted the opportunity to provide the most transparent and objective results. And this is possible only when the applicable legal framework puts the JICs in the condition of collecting high volumes of data for reliable and granular statistics: should an extensive interpretation of the consent requirement under Article 5(3) ePD and no exceptions be applied, the number of data will make the statistics less granular and less reliable and, therefore, the consequences for the media sector will be severe.

***

Article 5(3) ePD is not only ineffective in protecting data subjects' rights: it also left room to different interpretations of the consent requirement and its exceptions and, as a result, Article 5(3) ePD is not applied in the same way across the EU Member States.

We appreciate and are grateful for the efforts by the EDPB to provide a consistent interpretation; however, we believe that the Guidelines should not be used to extend the scope of application of Article 5(3), but rather to provide for a clear interpretation of the consent requirement in light of the latest technology developments and market trends, to give more certainty to data controllers which, in turn, will ensure higher protection of data subjects' rights and interests.

In other words: having been drafted by the EDPB, i.e. by all the European Data Protection Authorities, the Guidelines should take the opportunity to set shared and common solutions capable of ensuring that both business and individual needs are equally and properly taken into account, and protected.

Focusing efforts on extending the scope of application of the consent requirement would not only be ineffective, but also counterproductive. It has been proved that Article 5(3) has failed in ensuring data subjects' protection as, on the contrary, it has increased consent fatigue and compliance burdens for businesses: in light of the uselessness for individuals, there is clearly no reason to continue limiting business' rights and opportunities. The EDPB should contribute in finding a better strategy (even working together with other Authorities and Institutions) rather than reiterating a solution, consent, that proved to be ineffective.

Fedoweb
Presidente
Giancarlo Vergori

[16] See recital 45 of the "Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0457 .