

European Media Freedom Act: Rights of the media service providers (Article 4)

ARTICLE 19's concerns on the protection of journalists and journalistic sources from surveillance

The European Media Freedom Act (EMFA) is supposed to defend and enhance media freedom, independence and pluralism, and to establish common rules for the proper functioning and the preservation of the quality of media services across the EU. An essential component of this goal is to guarantee adequate protection of media service providers, and in particular of their independence and freedom.

Article 4 constitutes a welcome step in that direction. Indeed, we note that the protection of journalistic sources not only contributes to the right to freedom of expression and information and media freedom under Article 11 of the EU Charter of Fundamental Rights, but it is also a basic condition for press freedom. Without a high level of protection of journalistic sources "the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected"¹.

However, we note that the formulation of Article 4 fails to achieve this goal and needs to be improved. First, such formulation does not correspond to the protection of journalistic sources as provided in Article 10 European Convention of Human Rights (ECHR) and the relevant European Court of Human Rights (ECtHR) case law. We observe that the guarantees of source protection at the level of media service providers, producing and broadcasting news and journalistic content, should not be less than the guarantees of source protection that can be invoked by (individual) journalists in application of Article 10 ECHR.

Second, Recital 17 highlights the need to harmonise and further strengthen the protection at EU level. However, the suggested rules are vague, we need something clearer and stronger for the harmonisation to be achieved.

In particular, we flag that:

- Article 4(2)(b) does not guarantee an *ex ante* review by a judge, a court or another independent and impartial body, which is an essential requisite under international standards and the ECtHR case law.
- Article 4(2)(b) does not impose the criteria of necessity (no alternatives and interference must be crucial) and proportionality (no less intrusive measures available, interference in relation with seriousness of (preventing) crime) in cases where a disclosure order, sanction, search,

¹ See, among others: ECTHR, Goodwin v. the United Kingdom, judgment of 27 March 1996, § 39.

seizure, surveillance or inspection can be justified. Once more, this formulation does not comply with international standards and the relevant ECtHR case law.

- According to Article 4(2)(b) the prohibition on the Member State not to interfere with sources is only applicable "on the ground that they refuse to disclose information on their sources". However, we argue that this prohibition should be applicable in general, hence also in cases where the media service provider is not even aware of interception or (online) surveillance and has not refused disclosure. The new rules should unambiguously guarantee source protection also in such circumstances, in line with the relevant ECtHR case law.²
- Article (4)(2)(c) creates a legal basis for the deployment of spyware in any device or machine used by media service providers (and their employees) for reasons of national security and other serious crimes. However, we note that this happens without securing the guarantees of source protection that should also be upheld in application of Article 10 ECHR in this context, and in particular the *ex ante* review and the respect of the principles of necessity and proportionality highlighted above.

Our recommendations:

- Article 4 should provide protection to media service providers and (individual) journalists alike.
- Article 4(2)(b) should guarantee an *ex ante* review by a judge, a court or another independent and impartial body.
- Article 4(2)(b) should impose the criteria of necessity and proportionality in cases where a disclosure order, sanction, search, seizure, surveillance or inspection can be justified.
- The prohibition for Member States to interfere with sources under Article 4(2)(b) should be applicable in general, and thus also in cases where the media service provider or journalist is not aware of the surveillance and has not refused disclosure.
- The deployment of spyware in any device or machine used by media service providers (and their employees) for reasons of national security and other serious crimes should be subject to prior authorisation by a judicial authority and the respect of the principles of necessity and proportionality according to international and European human rights standards and relevant ECtHR case law.

²See ECtHR: Ernst ao v. Belgium, Tillack v. Belgium, Nagla v. Latvia, Standard Verlagsgesellschaft mbH v. Austria (no. 3), and Sergey Sorokin v. Russia).