RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0214 • articolo sottoposto a peer review • pubblicato in anteprima il 27 giu. 2025

Luigi Malferrari

New and reinforced rights for media service providers under Article 4 European Media Freedom Act

The free exercise of economic activity in the media sector is important both for the EU internal market and for the free media as a public watchdog. Article 4 of the European Media Freedom Act (EMFA) imposes on Member States the obligation to respect the media service providers' effective editorial freedom and independence. Article 4 EMFA protects in particular journalistic sources and confidential communications against both traditional forms of interference and spyware. The obligation of prior judicial authorization and a stringent justification and proportionality test are amongst the guarantees laid down in Article 4 EMFA. It "europeanizes" and "proceduralizes" the issues. It, furthermore, introduces a new guarantee consisting in an independent authority or body to provide assistance with regard to the exercise of the right to effective judicial remedy. Economic efficiency and the protection of the EU values are reconciled in Article 4 EMFA. Thus, the EMFA also strengthens the bond that holds individuals and society together in Europe.

Media service providers – Editorial freedom and independence – Internal market – Fundamental rights – EU values

Diritti nuovi e rafforzati per i fornitori di servizi media ai sensi dell'articolo 4 dello European Media Freedom Act

Il libero esercizio dell'attività economica nel settore dei media è importante sia per il mercato interno dell'Ue sia per la libertà dei media come "cane da guardia" pubblico. L'articolo 4 della legge europea sulla libertà dei media (EMFA) impone agli Stati membri l'obbligo di rispettare l'effettiva libertà editoriale e indipendenza dei fornitori di servizi mediatici. L'articolo 4 EMFA protegge, in particolare, le fonti giornalistiche e le comunicazioni riservate sia dalle forme tradizionali di ingerenza sia dallo spyware. L'obbligo di previa autorizzazione giudiziaria e un rigoroso test di giustificazione e proporzionalità rientrano tra le garanzie di cui all'articolo 4 dell'EMFA. Esso "europeizza" e "giuridifica" le questioni; introduce inoltre una nuova garanzia costituita da un'autorità o da un organismo indipendente per fornire assistenza nell'esercizio del diritto a un ricorso giurisdizionale effettivo. L'efficienza economica e la protezione dei valori dell'Ue trovano una riconciliazione nell'articolo 4. Pertanto, l'EMFA rafforza anche il vincolo che mantiene insieme gli individui e la società in Europa.

Fornitori di servizi mediatici – Libertà editoriale e indipendenza – Mercato interno – Diritti fondamentali – Valori dell'Ue

The Author is member of the Legal Service of the European Commission and lecturer at the Europa-Institute of the University of Saarland and at SciencesPo of the R. Schuman University of Strasbourg. The opinions expressed are purely personal

The Author thanks Maximilian Gerhold, Thomas Giegerich, Jan Kermer, Serena La Pergola, Audrius Perkauskas, Sofia Verza and Dirk Voorhoof for precious input. Any error of fact or law is attributable to the author only

This paper is part of the monographic section *EMFA under the spotlight: towards a common regulatory framework to foster media pluralism? – Part II* edited by Elda Brogi

1. Introduction

The media sector has dramatically changed in the last few decades. This change is still ongoing. Digitalization (including platformization) has been a major factor in the modernization and internationalization of the media, bringing with it new opportunities but also making the media sector increasingly complex and problematic[1]. This change has disrupted the traditional business model and the financial viability of media outlets as well as journalists' employment prospect[2]. The 2008 financial crisis has magnified these negative aspects, bringing further distress to the viability of the media and to the professional stability of journalists[3]. In addition, media freedom has been under strain, in particular due to the fact that governmental intervention and disinformation, including from third countries, have put into question the media public space in the EU[4]. Moreover, sensationalist and provocative content is often used to maximize engagement rates and advertising revenues and in turn it is amplified by the algorithms of Internet platforms[5]. The market power of Internet platforms is reinforced by the fact that only they have integrated ecosystems and the huge amount of data necessary for the optimal use of algorithms.

Against this backdrop, the European Media Freedom Act (EMFA) was enacted in the spring of 2024 after the Commission's proposal in September 2022[6]. The EMFA is in several regards a remarkable piece of EU legislation[7]. To begin with, the EMFA is the first piece of EU legislation that introduces a comprehensive regime for media services. It, thus, occupies a terrain that was traditionally understood as belonging to national legislation – understanding that was there despite the existence of the fundamental freedoms and

1. See the Explanatory Memorandum accompanying the Commission Proposal, COM(2022) 457, pp. 8-9; Council conclusions on safeguarding a free and pluralistic media system, § 21 (OJ of 7 December 2020, C 422/8); Reuters 2024.
2. Bayer 2024, p. 89.
3. *Ivi*, p. 91.
4. See also Raab 2022.
5. Council conclusions on safeguarding a free and pluralistic media system (2020), § 32.
6. 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 (COM/2022/457).
7. See also Cornils 2024.

of the Audio-Visual Media Services Directive[8]. Secondly, the EMFA is remarkable because it concerns one of the most sensitive aspects of our society: the media is a very special economic sector which is politically and culturally loaded, and at the same time, it constitutes a crucial aspect of our democracies due, inter alia, to its public watchdog function[9]. Not surprisingly, the EMFA has been denounced by some political, academic and economic constituencies, while it has been praised by journalist associations, liberal governments, NGOs and progressive academicians.

Within the EMFA, a special and central place is occupied by Article 4, which is titled "Rights of media service providers". Indeed, the protection of the media service providers' rights plays a crucial role in the EMFA ecosystem because this act aims at developing the internal media market and, at the same time, defending the pluralism and independence of the media (cf. Article 1 and recital 2 EMFA)[10]. According to the European Parliament's rapporteur for the EMFA, one of the most important achievements of the Act is the clear definition of safeguards for media providers, including public service broadcasters under Article 5 EMFA, against undue influence by Member States[11]. It is, thus, not surprising that Article 4 EMFA was probably the most debated provision during the legislative process, as the different versions by the Council and the European Parliament (EP) and the Commission's proposal testify[12].

In the present essay, the essential features of Article 4 EMFA are presented. Thereafter, I tackle the question of the extent to which Article 4 EMFA introduces a new normative approach or simply restates existing ones. In addition, the dispute regarding national security is deconstructed and the meaning of paragraph 9 of Article 4 EMFA is explained ("The Member States' responsibilities as laid down in the TEU and the TFEU are respected"). Furthermore, the issue of the EMFA's legal basis is examined. Finally, the future prospects of enforcement of Article 4 EMFA are discussed.

2. The content of Article 4 EMFA: how many rights, and for whom?

2.1. Article 4(1) EMFA: general clause with added normative value

Article 4 EMFA starts in paragraph 1 with a general proposition: "Media service providers shall have the right to exercise their economic activities in the internal market without restrictions other than those allowed pursuant to Union law". The provision lays down an individual's right, as the wording and the title of the provision indicate and as follows from the objective of the provision explained in particular in recitals 17 and 18 EMFA.

Article 4(1) EMFA might *prima facie* appear tautological: isn't the right to exercise the media service providers' economic activity in the internal market without restrictions already laid down in the freedom of establishment (Article 49 TFEU) and the freedom to provide services (Article 56 TFEU)? The answer is in the positive, however with an important caveat: the fundamental freedoms under the Treaty apply only where there is a cross-border element. By contrast, Article 4(1) EMFA bestows upon media service providers the right to exercise their economic activities in the internal market *tout court*, regardless of the presence of a cross-border element. Therefore, Article 4(1) EMFA is not purely declaratory in nature[13]. In secondary law, the EU legislator may set out rules

8. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).
9. See to this effect Bayer 2024, p. 96.
10. As regards the notion of pluralism see Jakubowicz 2015; Valcke–Picard–Dal Zotto 2015.
11. Verheyen 2024.
12. See in particular European Parliament IMCO's Opinion of 3 March 2023, 2022/0277(COD); European Parliament CULT Committee's Opinion of 31 March 2023, 2022/0277(COD); Council's text constituting the Mandate for negotiations with the European Parliament of 21 June 2023, 10954/23; European Parliament's draft position in view of the negotiation with Council adopted on 7 September 2023. See also Cornils 2024, under II, 1.
13. But see Ferreau 2024, p. 40.

that apply also in an intra-national context[14]. *En passant*, it should be noted that, since Article 4 EMFA particularizes the freedom of establishment and the freedom to provide services and given the absence of any indication to the contrary, the term "restriction" used in this provision should be given the same meaning as under Articles 49 and 56 TFEU: it is any measure emanating from the State or quasi-State authority or entities entrusted by the States where that measure is liable to prohibit, hinder or make less attractive the exercise of the media service providers' activity. That definition includes the measure that indirectly emanates from the State in the sense that the State uses a private party as *longa manus* of its action[15]. It is plausible that the term "restriction" in Article 4 EMFA also includes the measures enacted by associations capable of regulating the economic sector in a collective manner, which follows under certain conditions into the ambit of application of the fundamental freedoms[16]. That interpretation would follow from the need for harmony between Article 4 EMFA and the fundamental freedoms. It is an open question whether the ambit of application of Article 4 EMFA can include the deployment of spyware used by any private entity against journalists. Whereas that option has been advocated on the basis of valid policy considerations[17], it remains difficult to reach that result through legal exegesis.

Article 4(1) EMFA further provides that the media service providers' activities in the internal market is to be exercised "without restrictions other than those allowed pursuant to Union law". Is this clause stating only the obvious? If a national restriction is mandated by EU law (e.g. one of the obligations that Member States must apply regarding media market concentrations in compliance with Art. 22 EMFA; or a national measure imposed in compliance with the EU Unfair Commercial Practices Directive), it will qualify as being "allowed pursuant to Union law" in the meaning of Article 4(1) EMFA. By the same token, if a restriction is imposed by national authorities without being mandated by EU law, it needs to comply with the existing EU rules such as the freedom of establishment and the freedom to provide services. As a result, the restrictions to the economic activity of media service providers can be accepted only if they are either mandated or permitted under EU law. That is not superfluous because it clarifies the boundaries for Member States' intervention. It is also in line with the minimum harmonization clause laid down in Article 1(3) EMFA, because this clause provides for the possibility that Member States go further than the EMFA provisions however under the condition of higher protection for media pluralism or editorial independence. This is clarified in recital 8 EMFA, whereby "Member States should have the possibility to adopt more detailed or stricter rules in specific fields, provided that those rules ensure a higher level of protection for media pluralism or editorial independence in accordance with this Regulation and comply with Union law and that Member States do not restrict the free movement of media services from other Member States which comply with the rules laid down in those fields". Moreover, the last part of Article 4(1) EMFA has one additional function, namely to occupy the legislative ground in the field of media law; that may play a role in the assessment of the question of whether the Union has exercised in this field its legislative competence pursuant to Article 3(2) TFEU, which in turn determines the exclusive competence of the Union for the conclusion of an international agreement.

2.2. Article 4(2) EMFA: the protection of editorial freedom and independence of media service providers

Paragraphs 2 and 3 of Article 4 EMFA set out more specific rules than paragraph 1. They follow the 2-step scheme that is typical of the fundamental freedoms: first, a prohibition of principle and then, a derogation. The derogation is subject to numerous detailed conditions, which constitute the *plat de résistance* of the provision.

Paragraph 2 of Article 4 EMFA protects the editorial freedom and independence of media service providers. It is formulated as an obligation for the

14. Judgment of 30 January 2018, *Visser*, C-360/15, EU:C:2018:44, §§ 98-110.
15. See expressly recital 25 EMFA (*in fine*) as regards spyware.
16. Cf. judgment of 12 December 1974, *Walrave and Koch*, 36/74, EU:C:1974:140, § 17.
17. Kermer 2024-a.

Member States ("Member States shall respect…"). That circumstance however does not lead to the conclusion that it is not an individual's right for media service providers. Upon proper construction, it is in fact an individual's right. Indeed, to begin with, the title of Article 4 EMFA is "Rights of media service providers"[18]: the plural form ("Rights") indicates that there is more than one right laid down in the Article, i.e., more than the right expressly laid down in paragraph 1 of Article 4 EMFA. Then, the purpose of the provision is the protection of the editorial independence (see recital 17 EMFA). More precisely, the objective is "to put in place effective safeguards enabling the exercise of editorial freedom across the Union so that media service providers can independently produce and distribute their content across borders and recipients of media services can receive such content" (recital 18 EMFA). Furthermore, in EU law, individual rights can flow from obligations imposed on Member States, as is the case, for example, for the rights that are bestowed upon individuals by the free movement rules of the Treaty, which are addressed to the Member States[19]. In addition, a systematic element also indicates that Article 4 EMFA grants rights to individuals: since Article 4 EMFA specifies the content of the freedom of establishment and the freedom to provide services (which grant rights to individuals), the existence of rights of individuals should be recognized for Article 4 EMFA, too. Finally, still from a systemic viewpoint, Article 3 EMFA (the "sister" provision to Article 4 EMFA) must be taken into account. Under this provision, "Member States shall respect the right of recipients of media services to have access to a plurality of editorially independent media content and ensure that framework conditions are in place in line with this Regulation to safeguard that right, to the benefit of free and democratic discourse". Article 3 EMFA uses the same language as Article 4 EMFA ("Member States shall…") and its title clarifies that it is a right for the recipients of media services ("Right of recipients of media services")[20]. It is true that Article 3 EMFA in the Commission proposal used more explicit wording ("Recipients of media services in the Union shall have the right…"); however, the change in the formulation of the final text of Article 3 EMFA was done only to avoid the risk of creating an almost boundless obligation for media service providers. It has been objected that Article 3 EMFA does not create a subjective right[21]. However, it is arbitrary to consider, without any objective criterion, that some rights in EMFA are subjective whereas others are objective. Denying the existence of a right for individuals under Article 3 EMFA despite the clear title and the purpose of the provision is untenable in proper legal exegeses. That is underpinned by the systematic argument whereby Article 3 EMFA (like Article 4) specifies the content of the freedom of establishment and the free provision of services under the Treaty, which grant rights to individuals. Furthermore, it cannot be convincingly argued that Article 3 EMFA can be invoked only in combination with another provision of EMFA; in fact, there is no trace of that in the text of EMFA and, moreover, Article 3 EMFA alone entered into application on 8 November 2024, so that its solitary application must have some legal consequences; indeed, in EU law, where different interpretations[22] are possible, the one that preserves the normative value of the provision is to be preferred. What is more, Article 4 EMFA must be read in the light of the fundamental right to freedom of expression and freedom of the press under Article 11 Charter of Fundamental Rights; this provision constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the European Union is founded[23]. In light of the above, it must be considered that paragraph 2 of

18. Italic added.
19. See *ex multis* judgment of 7 February 1979, *Knoors v. Staatssecretaris voor Economische Zaken*, Case 115/78, EU:C:1979:31, § 20.
20. See Malferrari–Gerhold 2024.
21. Cf. Cole–Etteldorf (2024), p. 14. Cf. also Grandinetti 2024, § 5.
22. Cf. the pending case *Viktor Orbàn*, C-384/24.
23. Judgment of 4 October 2024, *Real Madrid v. Le Monde*, C-633/22, EU:C:2024:843, § 49.

Article 4 EMFA, as well as Article 3 EMFA, lay down individual rights proper.

With these clarifications made, it is important to emphasize that Article 4(2) EMFA finds its inspiration in the concept of *Staatsferne* ("distance from the State"). Under the first sentence of Article 4(2) EMFA, "Member States shall respect the *effective* editorial freedom and independence of media service providers in the exercise of their professional activities"[24]. The word "effective" indicates that it is not only the form but also the substance of the editorial freedom and independence that must be respected. This corresponds to a general approach in EU law which focuses on the substance of social and economic phenomena. What follows are the words "in the exercise of their professional activities", which is in keeping with the definition of media service providers, defined as "a natural or legal person whose *professional* activity is to provide a media service…"[25]. The word "professional" limits the definition to those persons who exercise the media activity in a sufficiently deontological and structured manner, thus excluding the improvised or spontaneous journalism that may exist sporadically in particular in the digital society[26]. Thus, the ambit of protected individuals is potentially more limited than those protected under Article 8 ECHR[27]. On the other hand, a profit aim is not necessary to fall into that definition because it is not required under the fundamental freedoms[28].

The second sentence of Article 4(2) EMFA specifies that "Member States, including their national regulatory authorities and bodies, shall not interfere in or try to influence the editorial policies and editorial decisions of media service providers". The term "editorial policies" covers any formal or informal strategy/direction (including guidelines) that a media service provider follows in its professional activity including the content direction of the media offer[29]. Then, the term "editorial decisions" refers to the specific decisions that are taken day-by-day in the exercise of the media profession, including in research, press room activities, investigation, selection, discussion and presentation. They comprise the choice of the topics, the prioritization, the style of presentation, the choice of the presenters and the selection of the guest speakers/writers[30]. According to Article 2, n° 8 of the Commission proposal, "editorial decision" means "a decision taken on a regular basis for the purpose of exercising editorial responsibility and linked to the day-to-day operation of a media service provider". A parallel can be drawn to Article 21 EMFA, whereby national measures that are liable to affect the editorial independence of media service providers can be accepted only under certain conditions. Further, Article 4(2) EMFA finds a pendant in Art. 6(3) EMFA, which protects the journalists' editorial independence and freedom from the media service providers' managers/owners.

The words "interfere in or try to influence" are quite broad, covering any activity that aims at hampering, limiting, affecting or domesticating the media. Indeed, the ways in which the State can, directly or indirectly, actually or potentially, try to exercise any form of influence over the media are varied and sometimes surreptitious[31]. According to recital 18 EMFA, such interference can be direct or indirect, from the State or other actors, including public authorities, elected officials, government

24. Italics added.

25. Italics added. See extensively Verza 2025.

26. For an example cf. judgment of 14 February 2019, *Buivids*, C-345/17, EU:C:2019:122 regarding Mr Buivids's video recording in a station of the Latvian national police and his publishing on Youtube of that video, which showed police officers going about their duties in the police station. In that case the CJEU had to interpret the notion of processing of personal data for journalistic purposes under Article 85 GDPR.

27. Cf. ECtHR's judgment of 8 November 2016, *Magyar Helsinki Bizottság v. Hungary*, n° 18030/11, § 168.

28. Judgment of 23 February 2016, *Commission v. Hungary* ("meal vouchers"), C-179/14, EU:C:2016:108, § 154. But cf. Brogi–Da Costa Leite Borges–Carlini et al. 2023, p. 50.

29. See also Ferreau 2024, p. 41.

30. *Ibidem*.

31. Cf. Trevisan–Štětka–Milosavljevič 2024.

officials and politicians, for example to obtain a political advantage[32]. There is, at the same time, the (legitimate) right of State officials to publicly criticize the work of the media, as long as it is done in a respectful and reasoned manner[33]. The line between the two phenomena may however be thin in practice.

The previous considerations highlight the particular significance of Article 4(2) EMFA. As clarified in the first sentence of recital 17 EMFA, "[t]he protection of editorial independence is a precondition for exercising the activity of media service providers and their professional integrity in a safe media environment. Editorial independence is especially important for media service providers which provide news and current affairs content, given its societal role as a public good". Editorial freedom and independence are essential for the proper functioning of the market and constitute a central feature of the media service: a media service produced without full editorial freedom and independence lacks quality. That is relevant for the internal market, as suggested by the first sentence of recital 16 EMFA which states that "[t]he free flow of trustworthy information is essential in a well-functioning internal market for media services". The State's interference in a media service provider's editorial independence places it at a competitive disadvantage because its services become qualitatively inferior to the services produced by a media service provider which enjoys full editorial independence. Therefore, the fact that a media service provider is - directly or indirectly, actually or potentially - interfered with in the exercise of its economic activity entails a restriction of its economic rights in the internal market and an uneven playing field. As stated in the second sentence of recital 17, "media service providers should be able to exercise their economic activities freely in the internal market and compete on an equal footing in an increasingly online environment where information flows across borders". Editorial freedom and independence of media are of course not only essential elements of the media service, they are also part of the guarantees enshrined in Article 11(2) Charter of Fundamental Rights. The abundant case law of the ECtHR testifies to this. Article 4(2) EMFA is, thus, a good example showing that the economic aspects are inextricably intertwined with the fundamental rights aspects. The previous considerations also play an important role in the debate regarding the legal basis, as is illustrated below.

Article 4 EMFA has been criticized on the ground that the EMFA does not provide for the specifications related to its enforcement[34]. However the details of the enforcement are usually not laid down in the text of regulations or directives, but provided for – as the case may be – in comitology acts; moreover, and in any event, the general clauses laid down in Article 288 TFEU ("A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States") and Article 4(3) TEU ("The Member States shall take any appropriate measure, general or particular, to ensure fulfillment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union") are usually considered to be the sufficient baseline for the obligation of enforcement by Member States[35].

2.3. Article 4(3) and (8) EMFA: the protection of journalistic sources and confidential communications and the right to effective judicial protection

2.3.1. The object of the protection

The protection of journalistic sources and confidential communications is the object of Article 4(3) EMFA whereby "Member State shall ensure that journalistic sources and confidential communications are effectively protected". The structure of the provision is analogue to that of Article 4(2) EMFA. The use of "ensure" underlines that it is an obligation of result for Member States. Member States must take all the legal and practical measures

32. See also Cole–Etteldorf 2023, p. 26.
33. See also Ferreau 2024, p. 42.
34. *Ibidem*.
35. See, to this effect, judgment of 30 March 2023, Case C-34/21, *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium*, EU:C:2023:270, § 77.

necessary for the effective protection of journalistic sources and confidential communications. For the same reasons illustrated above as regards Article 4(2) EMFA, this provision too lays down an individual's right. In this context it is to be asked whether the journalistic sources of the individual journalist are protected also *vis-à-vis* the owner of the media organization (in Germany this is called internal media freedom). The wording and the objective of the provision might be insufficient to support an answer in the positive.

The term "journalistic sources" comprises any information on facts and opinions which can be used by media service providers as the basis for a piece of news or an item of journalism. Recital 19 EMFA explains the economic significance of journalistic sources, which "are tantamount to 'raw material' for journalists: they are the basis for the production of media content by journalists, in particular news and current affairs content". As explained in recital 19 EMFA, "[i]t is therefore crucial that journalists' ability to collect, fact-check and analyse information be protected, in particular information imparted or communicated confidentially, both offline and online, which relates to or is capable of identifying journalistic sources". Journalistic sources are often confidential because, either for ethical or professional reasons, some individuals are willing to give information to journalists only under the condition of anonymity or confidentiality. If the anonymity or confidentiality of sources is destroyed, hampered or made less attractive, confidants will be discouraged from providing information to journalists so that the media service providers will have less "raw material" for producing their services, to the detriment of the free exercise of the media service activity.

Recital 21 EMFA emphasizes that the protection of journalistic sources is "crucial for safeguarding the 'public watchdog' role of media service providers, and particularly of investigative journalists, in democratic societies, and for upholding the rule of law". This corresponds to the ECtHR's case law, whereby "[t]he right of journalists to protect their sources is part of the freedom to 'receive and impart information and ideas without interference by public authorities' protected by Article 10 of the Convention and serves as one of its important safeguards. It is a cornerstone of freedom of the press, without which sources may be deterred from assisting the press in informing the public on matters of public interest"[36]. Without such protection, "the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information be adversely affected"[37]. Not only the publication, but also the preparatory steps to a publication, such as the gathering of information and the research and investigative activities of a journalist are inherent components of the freedom of the press, as enshrined in Article 10 of that Convention, and are, as such, protected[38]. In light of this case law and given the objective of Article 4(3) EMFA, the expression "journalistic sources" is to be interpreted broadly[39]. Indeed, in order to take account of the importance of the freedom of the press and the freedom of expression in media in every democratic society, it is necessary to interpret broadly concepts related to those freedoms[40].

The term "confidential communications" refers to any communication that because of its content or origin is imparted in a reserved manner and plays a role in the production/distribution of media content. Here again, given the liberal objective of the provision, this term is to be interpreted broadly.

Under Article 4(3) EMFA, the protection against State intervention is extended to persons who, because of their regular or professional relationship with a media service provider or its editorial staff,

36. ECtHR, judgment of 14 September 2010, *Sanoma Uitgevers B.V. v. the Netherlands*, Application n° 38224/03, § 50.
37. ECtHR, judgments of 27 March 1996, *Goodwin v. the United Kingdom*, Application n° 17488/90, § 39; of 29 June 2006, *Weber and Saravia v. Germany (dec.)*, Application n° 54934/00, § 143.
38. Judgment of 15 March 2022, *Autorité des marchés financiers*, C-302/20, EU:C:2022:190, § 68, with reference to ECtHR, judgments of 25 April 2006, *Dammann v. Switzerland*, § 52, and of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, § 128.
39. See also Ferreau 2024, p. 43.
40. *Autorité des marchés financiers*, cit., § 66.

might have relevant information[41]. This category is defined functionally, and, in view of its rationale, it is also to be interpreted broadly[42].

2.3.2. Three specific prohibitions for Member States

The second sentence of Article 4(3) EMFA specifies three types of measures which Member States shall not take. These three types of measures constitute restrictions to the free exercise of the media service provider activity. They are as follows:

a) to oblige media service providers or their editorial staff to disclose information related to or capable of identifying journalistic sources or confidential communications;
b) to detain, sanction, intercept or inspect media service providers or their editorial staff or subject them to surveillance or search and seizure;
c) to deploy intrusive surveillance software on media service providers.

The channels of communications between journalists and sources can thrive thanks to the digitalization, but are at the same time subject to new and invasive threats which are increasingly cross-border[43]. A risk for journalistic sources and confidential communications is particularly strong where, as is typically the case for spyware, the data are collected without the persons concerned being informed[44]. Going beyond this scenario, any risk, even of potential or indirect nature, for the sources or confidential communications is liable to lead to a chilling effect for the media[45]. Therefore, these three categories of prohibitions are to be construed broadly, i.e., rigorously. Orders to disclose sources potentially have a detrimental impact, not only on the source itself, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources, and on members of the public, who have an interest in receiving information imparted through anonymous sources[46]. It is irrelevant whether the media service providers are unaware of any detainment, sanction, interception or inspection taking place, because the condition of awareness is not laid down[47]. It is equally irrelevant whether the media service providers refuse disclosure or not because the potential negative effect on sources remains.

2.3.3. Derogation from the prohibitions under (strict) conditions

State intervention is, however, allowed under certain detailed conditions which are set out in the following paragraphs of Article 4 (i.e., paragraphs 4 and 5). According to Article 4(4) EMFA, one of the national measures listed above can be accepted only if it is:

a) provided for by Union or national law ("legality principle");
b) in compliance with Article 52(1) of the Charter and other Union law;
c) justified on a case-by-case basis by an overriding reason of public interest and proportionate;
d) subject to prior authorization by a judicial authority or an independent and impartial decision-making authority or, in duly justified exceptional and urgent cases, is subsequently authorized by such an authority without undue delay.

As regards the deployment of intrusive surveillance software (in short: spyware) referred to in point c) of Article 4(3) EMFA, two additional conditions for the derogation are laid down in paragraph 5 of Article 4 EMFA as follows:

– the measure is carried out for the purpose of investigating one of the persons referred to in paragraph 3, point (c), with regard to:

41. See also recital 20 EMFA.
42. See to this effect Ferreau 2024, p. 45.
43. Cf. Gerhardinger 2023, Section II.
44. See, by analogy, judgment of 21 December 2016, *Tele 2 Sverige and Watson*, joined cases C-203/15 and C-698/15, EU:C:2016:970, § 100.
45. Woodhams 2021, p. 18.
46. *Sanoma*, cit., § 89.
47. Voorhoof 2022, p. 3.

(i) offences listed in Article 2(2) of Framework Decision 2002/584/JHA punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least three years; or
(ii) other serious crimes punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least five years, as determined by the law of that Member State;

– one of the measures mentioned under points a) or b) would not be adequate and sufficient ("*ultima ratio*" or "subsidiarity rule").

Exceptions to rules are to be construed narrowly so that general rules are not negated[48]. In addition, according to the settled case-law of the ECtHR, exceptions to the freedom of expression are to be construed strictly and Article 10(2) ECHR leaves little scope for restrictions on freedom of expression in the fields of political speech and matters of public interest[49]. Therefore, all the abovementioned conditions shall be construed rigorously. As remarked by the Venice Commission, "[w]ith particular regard to journalism, it is well-established that surveillance tools may be applied in only the most exceptional circumstances. European and international sources have widely recognized that journalism's watchdog role requires exceptional caution when considering interferences with their functions"[50].

2.3.4. The derogation as codification of case law guarantees

By and large, the abovementioned conditions codify in substance the application of the general principles of EU law and/or existing rules under the ECHR, which are relevant pursuant to the synchronization provision laid down in Article 52(3) Charter. So, for example, the legality principle under letter a) entails that the legal basis authorizing the interference must define its scope and all the constituent elements sufficiently clearly and precisely[51]. Then, as regards the *ultima ratio* (or subsidiarity) rule laid down in Article 4(5) EMFA, under the case law of the ECtHR, if a Member State wishes to use intrusive surveillance software, it must be able to demonstrate that it is strictly necessary[52] and there are no less intrusive surveillance methods available to achieve the aim pursued[53]. The last part of Article 4(5) EMFA thus has the added value of clarifying and specifying the ambit of application of those principles and rules. Moreover, they make the guarantees applicable even in a purely domestic scenario, whereas the fundamental freedoms apply only in the presence of a cross-border element. In this context it should be added that the *ultima ratio* condition is part of the proportionality principle, which being a general principle of EU law applies to the whole of Article 4(3-5) EMFA. This means that searches and confiscations or other surveillance measures are unlawful if less intrusive measures are adequate and sufficient.

The obligation of prior authorization under Article 4(4)(c) EMFA, which was introduced during the negotiations, is particularly important in practice because it introduces the verification by an independent organ. Its absence in the Commission proposal was considered to be a lacuna because the obligation of prior authorization is a guarantee already provided for under Article 10 ECHR[54]. The ECtHR has indeed emphasized the importance of prior authorization by an independent organ for

48. Judgment of 28 October 2022, *HF and Generalstaatsanwaltschaft München*, C-435/22 PPU, EU:C:2022:852, § 120.
49. *Real Madrid v. Le Monde*, cit., § 53.
50. Venice Commission 2024, § 93.
51. See to this effect and by analogy *CG Bezirkshauptmannschaft Landeck*, cit., § 98 regarding the Law Enforcement Directive.
52. ECtHR, judgment of 12 January 2016, *Szabó and Vissy v. Hungary*, Application n° 37138/14, § 73, and judgment of 16 December 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy*, C-73/07, EU:C:2008:727, § 56; of 9 November 2010, *Volker und Markus Schecke*, joined cases C-92/09 and C-93/09, EU:C:2010:662, § 77.
53. See, by analogy, judgment of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, § 53.
54. See also Voorhoof 2022, p. 5.

interceptions of journalists[55]. The extension of the power of prior authorization to other independent authorities has been criticized on the grounds that they lack the same level of independence as the judicial branch, as they are part of the administrative branch of the executive power[56]. This criticism should be taken seriously; indeed, the ECtHR in *Sanoma* considered the public prosecutor's authorization to be incompatible with Article 10 ECHR because he/she was too much involved in the investigation and there was no pertinent authorization by an investigating judge[57]. But this criticism needs, at the same time, to be nuanced because in *Sanoma v. the Netherlands* the ECtHR found that the Member State involved (the Netherlands) had violated Article 10 ECHR inter alia on the ground that under the relevant Dutch legislation in terms of procedure the public prosecutor is a "party" defending interests potentially incompatible with journalistic source protection and can hardly be seen as objective and impartial so as to make the necessary assessment of the various competing interests[58]. A sufficient level of independence is instead required by Article 4(4)(c) EMFA. Indeed, that provision is to be construed in view of its protective objective and in consonance with the fundamental rights. This also finds expression in recital 21 EMFA, whereby "[i]n light thereof, ensuring an adequate level of protection for journalistic sources and confidential communications requires that measures for obtaining such information be authorised by an authority that can independently and impartially assess whether it is justified by an overriding reason of public interest, such as a court, a judge, a prosecutor acting in a judicial capacity, or another such authority with competence to authorise those measures in accordance with national law". The expression "another such authority" indicates that the authorities that may authorize the use of the restrictive measures at issue must have a level of independence and impartiality that is analogue to that possessed by a judicial organ. The prior authorization can be dispensed of only "in duly justified exceptional and urgent cases". The justification and urgency must be validly established before that exception can be used[59]. In any event it must remain exceptional.

2.3.5. The obligation of regular review of restrictive measures

Paragraph 6 of Article 4 EMFA further specifies that the abovementioned measures under b) and c) of Article 4(4) EMFA must be regularly reviewed in order to verify whether the conditions are still being met. This also corresponds in substance to the guarantees existing under the ECHR[60]. Given its purpose, it must be interpreted rigorously. It is an important provision in practice because otherwise the risk of overly long duration of the restrictive measures would be tangible.

2.3.6. The applicability of the Law Enforcement Directive

Paragraph 7 of Article 4 EMFA provides that the Law Enforcement Directive "shall apply to any processing of personal data carried out in the context of the deployment of the surveillance measures referred to in paragraph 3, point (b), of this Article or the deployment of intrusive surveillance software referred to in point (c) of that paragraph". It is unclear what the legal value of this provision is[61]. It could be asked whether it is purely declaratory in nature despite the use of the verb "shall". Indeed, pursuant to Article 1(1), the Law Enforcement Directive "lays down the rules relating to the protection of natural persons with regard to the processing of personal data by

55. Judgments of the ECtHR of 25 May 2021, *Big Brother Watch v. UK*, Applications nos. 58170/13, 62322/14 and 24960/15), §§ 351 et seq.; of 28 November 2024, *Klaudia Csikós v. Hungary*, Application n° 31091/16, §§ 53-54. See Voorhoof 2021; Voorhoof 2025.

56. Bayer 2024, p. 122.

57. ECtHR, judgment of 14 September 2014, *Sanoma v. the Netherlands*, Application n° 38224/03, § 100. See also Kermer 2024, p. 198.

58. *Sanoma*, cit., § 93.

59. See also, by analogy, *Tele 2 Sverige and Watson*, cit., § 120.

60. See to this effect ECtHR, judgment of 12 January 2016, *Szabó and Vissy v. Hungary*, Application n° 37138/14, § 26.

61. See also Ferreau 2024, p. 54.

competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". That said, the insertion of paragraph 7 of Article 4 EMFA may be explained by the legal uncertainty regarding the exact ambit of application of the Law Enforcement Directive. Such uncertainty stems in particular from the rather ambiguous recital 14 of that Directive, whereby "[s]ince this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive". This recital is of course to be read together with other parts of the Law Enforcement Directive such as Articles 13(3), 15(1) and 16(4), which indicate that Member State measures related to national security may fall into the ambit of application of the Directive[62]. Therefore, the legal uncertainty regarding the Directive was more perceived than real.

2.3.7. Judicial remedies and supportive independent authority/body

Paragraph 8 of Article 4 EMFA, in its first part, is about the remedies for media service providers. It has a declaratory nature, restating what already flows from Article 47 Charter of Fundamental Rights of the EU. Then, the second part of paragraph 8 of Article 4 EMFA provides that "Member States shall entrust an independent authority or body with relevant expertise to provide assistance to the persons referred to in the first subparagraph with regard to the exercise of that right". This authority/body will play an important role in upholding the rights of media service providers, as will be illustrated in detail below. The provision further specifies that "[w]here no such authority or body exists, those persons may seek assistance from a self-regulatory body or mechanism". This latter specification is a novelty in the provision because the words "shall entrust" in the previous sentence of Article 4(8) EMFA lay down an obligation and not an option for Member States to have in place an independent authority or body with relevant expertise. Legal provisions usually start from the premise that Member States comply with EU legal obligations, *a fortiori* where the obligation in question is laid down in the same legislative act. The sentence starting with "where no such authority exists" seems, by contrast, to explain what individuals can do in the event that the Member State concerned fails to comply with the abovementioned obligation to entrust an independent authority or body to provide assistance. The words "may seek assistance" could be construed as bestowing an individual's right upon the persons concerned.

2.4. The national security dispute

Paragraph 9 of Article 4 EMFA states, as already anticipated above, that "[t]he Member States' responsibilities as laid down in the TEU and the TFEU are respected". This terse provision is, as follows from recital 8, *in fine*, of the EMFA, a purely declaratory statement: it contains a mere description of what Article 4(2) TEU already does. Indeed, under this provision of the Treaty, "[t]he Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State".

Behind the very succinct wording of Article 4(9) EMFA lies a hard-fought debate in which two opposing camps were involved: on the one hand, the sovereigntists led by the French Ministry of Defense, which advocated for an outright carve-out in favor of national security[63], and, on the other hand, the journalist associations and NGOs,

62. See also by analogy *Tele 2 Sverige and Watson*, cit.

63. See *RSF urges French Interior Minister to abandon the national security exception in European Media Freedom Act* and *Hardline EU governments in late push to legitimise surveillance of journalists*.

which vehemently opposed any mention whatsoever of Member State powers in this field[64]. In the end, common sense has prevailed: a carve-out in favor of national security has been rejected because it would have deprived the whole Article 4(3) EMFA largely of any legal meaning and would have probably collided with the ECtHR's case law[65]. At the same time, there is a mention of the State powers albeit an innocuous one because it merely reiterates the content of Article 4(2) TEU[66]. In that regard, it corresponds to the solution chosen by the legislator in the NIS2 Directive[67] and starkly contrasts with the ominous recital imposed by the Council of the European Union in the AI Act, which has been rejected by the Commission in a declaration[68].

Article 4(2) TEU indicates that in the essential State functions of Member States, it is their exclusive responsibility to safeguard national security. The wording, purpose and context of the provision indicate that Article 4(2) TEU has a framing function and does not entail an exception to the application of EU law[69]. The CJEU held in the judgment *La Quadrature du Net* that "according to the Court's settled case-law, although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law"[70]. Although it is for the Member States to adopt appropriate measures to ensure law and order on their territory and their internal and external security, it does not follow that such measures *per se* fall outside the scope of European Union law. As the CJEU has held, "the only articles in which the FEU Treaty expressly provides for derogations applicable in situations which may affect law and order or public security are Articles 36, 45, 52, 65, 72, 346 and 347, which deal with exceptional and clearly defined cases. It cannot be inferred that the FEU Treaty contains an inherent general exception excluding all measures taken for reasons of law and order or public security from the scope of European Union law. The recognition of the existence of such an exception, regardless of the specific requirements laid down by the Treaty, might impair the binding nature of European Union law and its uniform application"[71]. This position is fully in line with previous case law from which the drafters of Article 4(2) TEU drew inspiration[72]. Therefore, measures adopted by Member States to safeguard national security, defense and public security are not, as such, excluded from the application of EU law solely because they are presented as being taken in the interest of national

64. As regards the various sources see Bayer 2024, p. 123.

65. See *Big Brother Watch v. UK*, cit.

66. See also, to this effect, Ferreau 2024, p. 53. But cf. Kermer 2024, p. 200.

67. Art. 2(6) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

68. Recital 24 of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

69. See Opinion of AG D. Spielman in Case C-448/23, *Commission v. Poland* ("judgments of the Polish Const. Court"), EU:C:2025:165, §§ 67-69 and 85-88.

70. Judgment of 6 October 2020, *La Quadrature du Net 1*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, § 99.

71. Judgment of 17 December 2020, *Commission v. Hungary* ("reception of applicants for international protection"), C-808/18, EU:C:2020:1029, § 214.

72. See, for example, judgments of 9 December 1997, *Commission v. France* ("Spanish strawberries"), C-265/95, EU:C:1997:595, §§ 33 to 35; of 11 January 2000, *Tanja Kreil v. Germany*, C-285/98, EU:C:2000:2, §§ 16 to 17; of 11 March 2003, *Alexander Dory v. Germany*, C-186/01, EU:C:2003:146, § 30; 8 April 2008, *Commission v. Italy* ("helicopters"), C-337/05, EU:C:2008:203, §§ 42-43; of 20 March 2018, *Commission v. Austria* ("State printing office"), C-187/16, EU:C:2018:194, §§ 75 to 78.

security[73]. In other words, national security is not a blank cheque that can be invoked by Member States to escape from their obligations under EU law[74]. Member States must comply with EU law even where they exercise an exclusive competence.

When taking measures to safeguard national security, Member States must be able to demonstrate, on the basis of sufficiently solid grounds, that they are confronted with a serious threat to national security which is shown to be genuine and present or foreseeable[75]. A Member State which wishes to avail itself of the derogations for the protection of its essential security interests must show that such a derogation is necessary in order to protect those interests[76]. It is for the Member State concerned to demonstrate these conditions, in particular that justification and proportionality are met. As regards, specifically, the condition that the provisions restricting internal market freedoms must be justified by one of the reasons listed in the Treaty or by an overriding reason in the public interest, it must be recalled that Member States must prove, in a concrete manner and by reference to the circumstances of the case, that those provisions are justified[77]. The ECHR imposes analogue limits to the use of security interests as a derogation to human rights[78].

The net result is that it is only under these conditions that Member States will be able to invoke national security to justify a derogation to the prohibition laid down in Article 4(3) EMFA; moreover, Member States will need to prove in a concrete, detailed and circumscribed manner with regard to the circumstances of the case that the conditions set out in paragraphs 4 and 5 of Article 4 EMFA are fulfilled and that the fundamental rights and the general principles of EU law (such as legal certainty and proportionality) are complied with.

2.5. Regulating spyware as the "major novum" under Art. 4 EMFA

It is worthwhile zooming in on spyware. Spyware comprises several types: for example, "underground spyware", commercially available spyware, and spyware developed by public authorities. In any form, spyware is one of the nightmares of privacy defenders; it has even been compared – not without ground – to a weapon[79]. From the opposite angle, it is a phenomenal investigative tool in the hands of public and private entities. Whereas the Commission's proposal used the term "spyware" as one of the defined terms, the final version of EMFA has preferred to use the term "intrusive surveillance software", which means "any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting or analysing data from such products or from the natural or legal persons using such products, including in an indiscriminate manner" (Article 2 n° 20 EMFA). The definition set out in the final version of the EMFA is arguably broader than the one in the Commission's proposal[80]. Indeed, it notably leaves out the terms "in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data or tracking activities across multiple end-user devices, without the natural or legal person concerned being made aware in a specific manner and having given their express specific consent in that regard". The definition in Article 2 n° 20 EMFA protects any type of data, including encrypted ones.

73. See in particular the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware Report of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)); Mildebrath 2022, p. 41.
74. But see, although without argumentation, Ferreau 2024, p. 54.
75. See, to this effect, *La Quadrature du Net 1*, cit., § 137.
76. *Commission v. Austria* ("State printing office"), cit., § 78.
77. Judgment of 18 June 2020, *Commission v. Hungary* ("NGOs"), C-78/18, EU:C:2020:476, § 77.
78. European Court of Human Rights 2022, pp. 61-65.
79. Phillips 2023, p. 5.
80. Kermer 2024, pp. 198-199.

The spyware matter has been brought to the attention of public opinion, inter alia, through several scandals including the so-called Pegasus scandal from 2021, referring to the notorious software "Pegasus" produced by the Israel-based NOS group[81]. Several opinions, reports, debates, studies and recommendations have followed[82]. On 16 October 2023 the Parliamentary Assembly of the Council of Europe declared in a resolution that the secret surveillance of political opponents, public officials, journalists, human rights defenders and civil society for purposes other than those listed in the European Convention of Human Rights, such as preventing crime or protecting national security, would be a clear violation of the Convention. According to the Venice Commission of the Council of Europe, "the potential for unjustified or disproportionate intrusive surveillance using such a tool is significant. If left unregulated, spyware is a potent surveillance weapon that can be used to curtail human rights, censor and criminalise criticism and dissent and harass (or even suppress) journalists, human rights activists, political opponents and repress civil society organisations"[83]. It further held that "[t]he Pegasus scandal showed that journalists were apparently being targeted simply because they are journalists, which is unacceptable in a democratic society"[84]. Substantial forensic reporting by civil society organizations – such as Citizen Lab, Amnesty Tech, and AccessNow – has identified significant evidence of abusive surveillance using spyware technologies[85].

There are two extraordinary things about spyware. First, its pervasiveness and sophistication: as Bill Marczak of Citizens Lab recalled during his testimony at the PEGA Committee of the European Parliament, spyware is not only a tool for listening in and abducting data, but is also capable of doctoring documents, changing preferences of the device and activating tools of the targeted device such as the camera or other apps. Second, its ease of use is remarkable: Bill Marczak explained that, once you buy a license to use Pegasus for a specific country, you merely need to dial in the telephone number you want to target, and that is sufficient to put it under surveillance (so-called "zero-click spyware"). As noted by the Venice Commission, "technical developments make surveillance 'easier and easier to use'"[86]. Spyware yields thus an unprecedented level of intrusion thanks to its powerful technological sophistication. Spyware such as Pegasus should not be equated with "traditional" law enforcement interception tools; rather, it appears to be more similar to "government Trojan" or "online searches" solutions that had in the past raised serious legal concerns[87].

Accordingly, the use of spyware constitutes a major challenge to the rule of law, fundamental rights and values of the EU, which "define the very identity of the European Union as a common legal order"[88]. That is particularly true for the media. As clarified in recital 25 EMFA, intrusive surveillance software "has dissuasive effects on the free exercise of economic activities in the media sector. It jeopardises, in particular, the trusted relationship of journalists with their sources, which is the core of the journalistic profession. Given the digital and intrusive nature of such software and the use of devices across borders, it has a particularly detrimental impact on the exercise of economic activities by media service providers in the internal market. It is therefore necessary to ensure that media service providers, including journalists, operating in the internal market for media services can rely on robust harmonised protection in relation to the deployment of intrusive surveillance software in the Union, including where Member State authorities resort to private parties to deploy

81. See Mildebrath 2022, p. 41; Kermer 2024-a. See also Reuters 2025.

82. For a list see Venice Commission 2024, §§ 31-33. See also Vidal Marti 2023.

83. Venice Commission 2024, § 12.

84. *Ivi*, § 96.

85. *Ivi*, § 12.

86. *Ivi*, § 14.

87. European Data Protection Supervisor 2022, p. 4.

88. Judgment of 16 February 2022, *Hungary v. EP and Council* ("Conditionality Reg."), C-156/21, EU:C:2022:97, § 127.

it"[89]. This is also relevant for the issue of legal basis, which is discussed below.

That said, we live in a world where criminal threats are challenging and increasingly sophisticated. Spyware can be used by law enforcement authorities to put nefarious and technically adept criminals under surveillance. This can be done also cross-border through the cooperation of authorities from different Member States: an example thereof can be drawn from the Case C-670/22, *Staatsanwaltschaft Berlin v. M.N.* Thus, spyware can also be used to benefit legitimate societal goals. Indeed, Member States have a national security responsibility under Article 4(2) TEU and a competence for the maintenance of law and order (cf. Article 72 TFEU).

The balancing of these conflicting needs is a very delicate exercise, which the legislator has achieved in Article 4 EMFA. It is the result of the confrontation between two opposing camps which emerged in the legislative process of the EMFA with regard to Article 4. Whereas the European Parliament pushed for far-reaching protection against intrusive surveillance software, the Council (in particular some Member States) had a more cautious approach[90]. The solution adopted by the EU legislator in Article 4 EMFA strikes a good balance, by relying in substance on the guarantees provided by the Charter of fundamental rights of the EU, the general principles of EU law, the ECHR and the Convention 108[91]. EMFA, thus, needs to be put into the context of the already existing fundamental rights guarantees and general principles of EU law.

In its case law, the ECtHR has worked out a number of guarantees to protect individuals from secret surveillance by the State, such as: the State's obligation to set out the circumstances and the conditions upon which public authorities may resort to surveillance measures; the obligation to define the categories of individuals who can be subject to surveillance; the obligation to set a limit on the duration of surveillance; the obligation to determine the procedure that needs to be complied with when examining, using, and storing the data obtained; the obligation to take precautions when communicating the data to other parties; the obligation to specify the circumstances under which the obtained data must be erased or destroyed[92].

The list of crimes that is set out in Article 4(5)(b)(ii) EMFA, which has been criticized for being excessively broad[93], raises an issue which however must be relativized in its practical consequences because that provision must be interpreted in compliance with the EU fundamental rights and the general principles of EU law. Under the CJEU's case law, in compliance with the principles of necessity and proportionality, the seriousness of the intrusion can be justified only by the seriousness of the public interest that is pursued by the public authorities[94]. This corresponds in substance to the ECtHR's case law[95], whereby the higher the level of interference, the more robust the level of safeguards must be[96]. In *La Quadrature du Net II*, the CJEU used the terms "serious and even 'particularly serious' interferences with the fundamental rights concerned" when referring to national measures allowing general access to all retained traffic and

89. See also ECtHR, decision of 8 December 2005, *Nordisk Film & TV A/S v. Denmark*, Application n° 40485/02; *Sanoma*, cit., § 65.

90. See Ferreau 2024, p. 51.

91. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n° 108, 2018).

92. ECtHR, judgments of 24 April 1990, *Huvig v. France*, Application n° 11105/84, § 34; of 29 June 2006, *Weber and Saravia v. Germany (dec.)*, Application n° 54934/00, § 95; and of 11 January 2022, *Association for European Integration and Human Rights and Ekimdzhiev and Others v. Bulgaria*, Application n° 70078/12, § 76.

93. Kermer 2024, p. 202.

94. *La Quadrature du Net II*, cit., 95. See also, by analogy, *Tele 2 Sverige and Watson*, cit., § 102.

95. See, to this effect, Ferreau 2024, p. 47.

96. Judgments of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, §§ 116-117; of 8 December 2022, *Orde van Vlaamse Balies*, C-694/20, EU:C:2022:963, § 41.

location data[97]. The seriousness of the offence is one of the main parameters in assessing the proportionality of the interference that accessing the personal data contained in a mobile telephone represents[98]. In light of the findings made by the PEGA Committee of the European Parliament and of the abovementioned report by the Venice Commission[99], the interference with fundamental rights by spyware is usually extremely serious[100]; that is all the more so that it cannot be ruled out that the data contained in a device such as a mobile phone may include particularly sensitive data[101]. The corollary is that the public interest that needs to be invoked to justify the use of spyware must also be very serious, i.e., that the seriousness of the offence pursued must be particularly high, accordingly. It is true that the CJEU, when interpreting the Law Enforcement Directive, held that to consider that only combatting serious crime may justify access to data contained in a mobile telephone would limit the investigative power of the competent authorities and that would increase the risk of impunity of such offences[102]. However, that judgment was handed down in a case regarding a "normal" access to a phone data and not access through spyware. Moreover, the judicial dictum regarding the correspondence between the seriousness of the intrusion and the seriousness of the objective pursued belongs to settled case law of the CJEU. It follows that the Member States cannot distort the concept of "serious offence" and, by extension, that of "serious crime", by including within it, for the purposes of applying the derogation under Article 4(5) EMFA, offences which are manifestly not serious offences, in the light of the societal conditions prevailing in the Member State concerned, even though the legislature of that Member State has provided for such offences to be punishable by a maximum term of imprisonment of five years[103]. Moreover, the fact that a journalist's conduct falls into the category of the crimes listed in Article 4 EMFA is alone insufficient to justify the deployment of spyware; in fact, additional requirements must be fulfilled, including proportionality in concreto (see below), so that judicial or independent authorities must refuse the authorization of the restrictive measure if the offence at issue is manifestly not serious[104].

The obligation of justification entails that Member State authorities must prove that the use of spyware is justified by an overriding reason of public interest with regard to one of the crimes listed in Article 4(5) EMFA. The terms "overriding reason of public interest" is an EU law concept, so that Member States authorities cannot define it *ad libitum*: they can invoke it only where the public interest is sufficiently clearly defined and fulfills the criteria set out in the EU case law. In view of the wording in the German version of Article 4(4) (c) EMFA, the opinion has been expressed that this provision requires a mere balancing of the different interests and not a strict necessity examination[105]. It is, however, not clear whether the German version would imply a more lenient verification of the justification requirement. Moreover, and in any event, this opinion overlooks the fact that other versions such as the English, French, Italian and Spanish ones use the usual expression ("overriding reasons of public interest", "raisons impérieuses d'interêt général", "motivo imperativo

97. Judgment of 30 April 2024, *La Quadrature du Net II*, Case C-470/21, EU:C:2024:370, § 128.

98. See, by analogy, judgment of 4 October 2024, *CG v. Bezirkshauptmannschaft Landeck*, C-548/21, EU:C:2024:830, § 96 regarding the Law Enforcement Directive.

99. Venice Commission 2024, § 9. See also European Data Protection Supervisor 2022, p. 8 whereby "[t]he level of interference with the right to privacy is so severe that the individual is in fact deprived of it".

100. *Tele 2 Sverige and Watson*, cit., § 100.

101. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., §§ 94-95 and 107 regarding the Law Enforcement Directive.

102. *CG v. Bezirkshauptmannschaft Landeck*, cit., § 97.

103. See, by analogy, judgment of 30 April 2024, *Procura di Bolzano*, C-178/22, EU:C:2024:371, § 50.

104. See, by analogy, *Procura di Bolzano*, cit., § 62. See also, to this effect and by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 105 regarding the Law Enforcement Directive. See Palmiotto 2024.

105. Ferreau 2024, p. 46.

d'interesse generale" and "una razón imperiosa de interés general") which is also used in other pieces of EU legislation (e.g., the Services Directive) as well as in the CJEU's case law regarding the justification of restrictions to free movement under the Treaty. In addition, the principle of proportionality, being a general principle of EU law, applies in the context of the application of secondary law such as Article 4(4)(c) EMFA. It must also be understood in accordance with the concept/condition of "an overriding requirement in the public interest" and the inherent (procedural) guarantees as developed in the case law of the ECtHR on the protection of journalistic sources. Therefore, it is well-founded to consider that a full justification and necessity examination must be conducted under Article 4(4)(c) EMFA. In that regard, the measure adopted must correspond genuinely and strictly to the objective of investigation set out in Article 4(5) EMFA[106]. The Member State must prove in a concrete manner and by reference to the circumstances of the case, that the measure is justified[107]. Therefore, it cannot be validly considered that the EU legislator has *en bloc* justified or even blessed the use of spyware by national authorities. The compliance with Article 4 EMFA of the use of spyware depends on a number of strict conditions which must be proved according to the burden of proof set out in EU law: it is only under the proviso that the use of spyware, in a specific case (not *en bloc*!) may possibly be compatible with the EMFA. In particular, politically motivated surveillance is certainly incompatible with Article 4 EMFA because it does not qualify as a valid justification.

In this context it must be emphasized that the test of proportionality, which is a general principle of EU law and whose observance is recalled in Art. 4(4) EMFA, plays a very important (often crucial) role in practice. In accordance with that principle, the surveillance measure, including its duration and scope, shall not exceed what is necessary to achieve the (legitimate) objective pursued[108]. This requires balancing, on the one hand, the need to combat one of the serious crimes listed in Article 4(5) EMFA and, on the other hand, the seriousness of the interference with an individual's right to data protection and private life[109]. Recital 26 EMFA, by relying on the case law, explains in detail what the principle of proportionality entails. It states that "[a]ccording to the principle of proportionality, limitations can be made to an individual's rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union. Thus, as regards specifically the deployment of intrusive surveillance software, it is necessary to ascertain whether the offence in question attains a threshold of seriousness as laid down in this Regulation, whether, following an individual assessment of all the relevant circumstances in a given case, the investigation and prosecution of that offence merit the particularly intrusive interference with fundamental rights and economic freedoms consisting in the deployment of intrusive surveillance software, whether there is sufficient evidence that the offence in question has been committed, and whether the deployment of intrusive surveillance software is relevant for the purpose of establishing the facts related to the investigation and prosecution of that offence"[110]. This constitutes detailed and precious guidance for the national authorities, in particular the judiciary, in the application of Art. 4 EMFA.

When interpreting secondary law such as Article 4 EMFA, national authorities must take account of the fundamental rights such as liberty and security, private and family life, privacy, free-

106. See, by analogy, *La Quadrature du Net II*, cit., § 67 as regards Article 15(1) of Directive 2002/58.

107. Judgments of 18 June 2020, *Commission v. Hungary* ("usufruct"), C-235/17, EU:C:2020:476, § 77; *Commission v. Hungary* ("NGOs"), cit., § 77.

108. See also Article 5 of Convention 108 and ECtHR, judgment of 2 September 2010, *Uzun v. Germany*, Application n° 35623/05. The ECtHR found that a GPS device for location tracking was a less intrusive measure than the interception of personal communications.

109. See, by analogy, *La Quadrature du Net I*, cit., § 131.

110. As regards the need for evidence, in the context of the interpretation of Law Enforcement Directive the CJEU has required the existence of reasonable suspicions is supported by subjective and sufficient evidence (*CG v. Bezirkshauptmannschaft Landeck*, cit., § 101).

dom of expression, and freedom and pluralism of the media, enshrined respectively in Articles 6, 7, 8, 11(1) and 11(2) Charter of the fundamental rights of the EU[111]. The interpretation of relevant secondary law must take account of the importance of the right to freedom of expression, which constitutes one of the essential foundations of a pluralistic, democratic society, and is one of the values upon which, under Article 2 TEU, the Union is founded[112]. Spyware interferes not only with freedom of expression and freedom of the media, but also with the rights of both journalists and third parties to privacy and to private life; this reinforces the need for a particularly limited use of such measures and the requirement of very precisely developed provisions[113]. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 ECHR[114]. The protection of the fundamental right to respect for private life at EU level requires that derogations and limitations on the protection of personal data are to apply only in so far as is strictly necessary[115]. The ECtHR specified that the right to privacy would be "unacceptably weakened if the use of modern technologies in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such technologies against important private-life interests"[116]. The particular context in which the interference with fundamental rights takes place, in particular the modalities of the intrusion and the amount of data obtained, cannot be ignored in the analysis[117]. One of the findings in the interesting report published in April 2023 by the UN Human Rights Council and drafted by special rapporteur Prof. Fionnuala Ní Aoláin of the University of Minnesota Law School is that there may well be a category of spyware which, by virtue of its indiscriminate and disproportionate impact, can never be operated in a lawful manner[118]. It can be inferred from Article 11 Charter of Fundamental Rights a positive obligation for Member States to avoid lacunae in the security of IT systems concerned, just like Member States are pursuant to Article 10 ECHR under a positive duty to set up a legal framework to ensure effective media pluralism[119].

A further general principle of EU law is legal certainty. According to that principle, individuals must have access to the relevant legal rules (including those governing the use of surveillance measures) and must be able to anticipate the consequences of their application[120]. The law must indicate the limits to discretion conferred on the authorities and the criteria according to which it is exercised with sufficient clarity in order to give to individuals adequate protection against arbitrary interference[121]. The principle of legal certainty requires that EU or national rules are clear, precise

111. See, by analogy, *La Quadrature du Net II*, cit., § 68.

112. See, to this effect, *La Quadrature du Net II*, § 68.

113. Cf. Cole–Etteldorf 2023, p. 28.

114. ECtHR, judgment of 4 December 2008, *S. and Marper v. the United Kingdom*, Applications n° 30562/04 and 30566/04, § 103.

115. *Tele 2 Sverige and Watson*, cit., § 96.

116. ECtHR, Judgment of 13 February 2023, *Podchasov v. Russia*, Application n° 33696/19, § 62.

117. See, by analogy, *La Quadrature du Net II*, cit., § 107 as regards Article 15(1) of Directive 2002/58.

118. Ní Aoláin 2023.

119. ECtHR, judgment of 7 June 2012, *Centro Europa 7*, application n° 38433/09, § 134. See also, by analogy, Order by the German Constitutional Court of 8 June 2021, *1 BvR 2771/18*, § 32.

120. See, to this effect, judgment of 10 March 2009, *Proceedings brought by Heinrich*, C-345/06, EU:C:2009:140, § 44. ECtHR, judgments of 18 May 2010, *Kennedy v. the United Kingdom*, Application n° 26839/05, § 151 of 4 May 2000, *Rotaru v. Romania*, Application n° 28341/95, § 52; of 1 July 2008, *Liberty and Others v. UK*, Application n° 58243/00, § 59; and of 10 February 2009, *Iordachi and Others v. Moldova*, Application n° 25198/02, § 37.

121. See, to this effect, judgment of 4 June 2002, *Commission v. France* ("Elf-Aquitaine"), C-483/99, EU:C:2002:327 § 50; ECtHR, judgments of 6 December 2007, *Liu v. Russia*, Application n° 58149/09, §§ 92 and 98; of 4

and predictable as regards their effects, in particular when they may have unfavorable consequences for private individuals and undertakings[122]. When public authorities act within the scope of EU law, they must exercise their discretion on the basis of objective, non-discriminatory, sufficiently specific and clear criteria known in advance[123].

Under Article 4(5)(b) EMFA, the deployment of spyware must be carried out "for the purpose of investigating one of the persons referred to in paragraph 3, point (c)". This wording indicates that spyware can be used against a given target only to investigate a crime that has been likely committed by him/her and not by other individuals[124]. This interpretation is also in line with the objective of the provision, which is to offer a "robust harmonized protection in relation to the deployment of intrusive surveillance software in the Union" (recital 19 EMFA), and with the fundamental rights of journalists.

The secret nature of surveillance serves, to a certain extent, a functional purpose in the investigations, but collides with an individual's rights such as the right of defence. The right for individuals to be notified that they were subject to the use of surveillance is recognized in the case law as being instrumental to enable the affected individuals to exercise their right to the protection of personal data and to privacy as well as their right to an effective judicial remedy[125]. This is recognized in recital 22 of EMFA whereby "in line with the established case law of the European Court of Human Rights, the right to effective judicial protection presupposes, in principle, being informed in due time, without jeopardising the effectiveness of ongoing investigations, of the surveillance measures taken without the knowledge of the person concerned in order to effectively exercise that right"[126]. The limitations of the right to notification in due time must be provided for by law, respect the essence of the rights and freedoms at issue and, in compliance with the principle of proportionality, must be necessary and genuinely meet the legitimate objective of general interest or the need to protect rights and freedoms of others[127]. In a case regarding an individual who was considered to constitute a terrorist threat, the CJEU held that the competent authorities (i.e., those that requested the measure) must notify him as soon as the notification no longer jeopardizes the investigation, so that the individual can exercise his rights under Articles 7, 8 and 47 of the Charter[128]. In a similar vein, the ECtHR ruled, in a case regarding the use of a surveillance measure, that the notification is to take place once the risk has evaporated[129]. It is unclear when exactly the notification to the target is to take place; there will be the need for clearer criteria to be worked out in the case law, in order to limit the public authorities' discretion.

The abovementioned report by Prof. Fionnuala Ní Aoláin pointed out that victims of unlawful surveillance must have the knowledge and the

December 2015, *Roman Zakharov v. Russia*, Application n° 47143/06, § 230 and 247. See also Article 8 of the Law Enforcement Directive.

122. Judgment of 5 July 2012, *SIAT*, C-318/10, EU:C:2012:415, § 58.

123. Judgments of 10 March 2009, *Hartlauer*, C-169/07, EU:C:2009:141, § 64; of 14 March 2000, *Association Église de Scientologie de Paris*, C-54/99, EU:C:2000:124, § 22; *Commission v. France* ("Elf Aquitaine"), cit., § 50.

124. Indication given by Christoph Brill during the EMFA talk "Safeguarding journalistic sources under Article 4 of the European Media Freedom Act", held on 13 January 2025 at the European University Institute.

125. *Tele 2 Sverige and Watson*, cit., § 121; *La Quadrature du Net 1*, cit., § 190. See also ECtHR, judgments of 4 December 2015, *Roman Zakharov v. Russia*, Application n° 47143/06, § 287; of 28 November 2024, *Klaudia Csikós v. Hungary*, Application n° 31091/16, § 60.

126. See also, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., §§ 117 et seq. regarding the Law Enforcement Directive.

127. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 120 regarding the Law Enforcement Directive.

128. *Ibidem*. For example, to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased and to avail themselves of an effective remedy before a tribunal (*La Quadrature du Net*, § 190).

129. *Roman Zakharov v. Russia*, cit., § 287. See also Voorhoof 2025.

means to use litigation to hold spyware producers to account. Accordingly, not only the existence of the measure, but also the grounds on which the authorization is based, must be notified to the target[130]. National legal rules which exclude, as a general rule, any right to obtain such information are not consistent with EU law[131]. The CJEU ruled that "[t]he right to an effective judicial review, guaranteed by Article 47 of the Charter, requires that the person concerned must be able to ascertain the reasons for a decision taken in relation to him or her, either by reading that decision or by being informed of those reasons, so as to enable him or her to defend his or her rights in the best possible conditions and to decide in full knowledge of the facts whether or not to refer the matter to the court with jurisdiction to review the lawfulness of that decision"[132]. It also held that "once the person concerned has been informed that special investigative methods have been applied to him or her, the obligation to state reasons referred to in the second paragraph of Article 47 of the Charter requires that that person be (…) in a position to understand the reasons why the use of those methods has been authorised, in order to be able, where appropriate, to challenge that authorisation appropriately and effectively"[133].

The judicial or quasi-judicial *ex ante* authorization laid down in Article 4(4)(d) is a guarantee that is essential where the risk of interference with the data subject's rights is serious or even very serious[134]; it plays a very important role in practice, as already mentioned above. Under the ECtHR case law, such authorization must be obtained by the authorities in order to subject the media to secret surveillance measures[135]. The requisite review is to be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not[136]. The court or independent administrative body entrusted with carrying out the prior review must have the power to strike a fair balance between, on the one hand, the legitimate interests relating to the needs of the investigation and, on the other hand, the fundamental rights of the persons concerned[137]. If that review is carried out not by a court but by an independent administrative body, that body must have a status that enables it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence; accordingly, it follows that the requirement of independence that has to be satisfied by the body entrusted with carrying out the prior review means that that body must be a third party in relation to the authority which requests access to the data, so that the former is able to carry out the review objectively and impartially and free from any external influence; in particular, in the criminal field, the requirement of independence entails that the body entrusted with the prior review, first, is not to be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-à-vis the parties to the criminal proceedings[138].

The rule of *ex ante* authorization is very important also because it "europeanizes" and "proceduralizes" the issues, by enabling (if it is a court of last instance, by obliging) the judicial organ to make a reference to the CJEU, which constitutes an additional procedural safeguard. The rule of *ex ante* authorization, however, has a limit: in

130. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 120 regarding the Law Enforcement Directive.
131. *Ivi*, § 121.
132. Judgment of 16 February 2023, *HYA*, C-349/21, EU:C:2023:102, § 46.
133. *Ivi*, § 55.
134. See, by analogy, *CG v. Bezirkshauptmannschaft Landeck*, cit., § 102 regarding the Law Enforcement Directive.
135. ECtHR, judgment of 22 November 2012, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, Application n° 39315/06, § 101.
136. ECtHR, judgment of 30 August 2022, *Sorokin v. Russia*, Application n° 52808/09, § 46.
137. See, by analogy, judgment *La Quadrature du Net II*, cit., § 125 as regards Article 15(1) of Directive 2002/58.
138. *Ivi*, § 126.

justified cases, the review can take place after the deployment of the surveillance measures[139]. But this exception comes with two caveats: i) the authorization must take place within a "short time"[140] and ii) there must be sufficient guarantees that the exception is used sparingly and only in duly justified cases[141]. In a case regarding surveillance on a journalist, the ECtHR importantly held that the review is to be done at the latest before the access and use of the obtained materials by the public authorities[142]. This exception to this *ex ante* authorization has been criticized for being a possible loophole[143]. It is indeed a risky provision, which is to be interpreted very narrowly precisely because otherwise the main rule would be easily and fully frustrated.

As regards the obligation of recurrent review (which is laid down in Art. 4(6) EMFA), it is noteworthy that the ECtHR held that an assessment is to be made at each stage of the process of the necessity and proportionality of the surveillance measures, namely not only at the moment of the assessment for authorising the measure but also during its execution and thereafter[144]. The case law has specified that when performing the assessment, the court or the independent administrative authority must understand the implications of the surveillance technique used, the nature of the intrusive surveillance software including its relevant technical features, and consider whether its deployment can be limited to certain individuals or groups of individuals[145]. Furthermore, the court or the independent administrative authority must have full and unfettered access to all necessary information, including confidential materials, and that the officials involved in interception activities have a duty to disclose to it any material it requires[146].

In its review of the use of intrusive surveillance software, the judicial or quasi-judicial authority must be able to examine all relevant questions of law and fact for carrying out a proper review of the measure[147]. The individual's right to an effective remedy entails the right to inspect and comment on evidence and observations before the court[148]. This right may be limited by an overriding reason of public interest: the competent organ must verify whether the reasons for the non-disclosure are well-founded[149]. In instances where the ECtHR found the non-disclosure to be justified, and therefore the adversarial principle is limited, it must be counterbalanced by procedural safeguards[150], en-

139. *La Quadrature du Net 1*, cit., § 189; see also ECtHR judgment of 12 January 2016, *Szabó and Vissy v. Hungary*, Application n° 37138/14, § 76 and 81.

140. *La Quadrature du Net 1*, cit., § 189; see also ECtHR, *Szabó and Vissy v. Hungary*, cit., §§ 76 and 81.

141. *Roman Zakharov v. Russia*, cit., § 266.

142. ECtHR, judgment of 14 September 2010, *Sanoma Uitgevers B.v the Netherlands*, Application n° 38224/03, § 91; *Big Brothers v. UK*, cit. See also Voorhoof 2021.

143. Kermer 2024, p. 199.

144. ECtHR, judgment of 6 September 1978, *Klass v. Germany*, Application n° 5029/71, § 55.

145. See for example, *Szabó and Vissy v. Hungary*, cit., § 77.

146. *Roman Zakharov v. Russia*, cit., § 281.

147. Judgment of 16 November 2023, *Ligue des droits humains ASBL, BA v. Organe de contrôle de l'information policière*, C333/22, EU:C:2023:874, §§ 67-69; ECtHR, judgments of 11 June 2019, *Ozdil and Others v. the Republic of Moldova*, Application n° 42305/18, § 68; 15 November 1996, *Chahal v. the United Kingdom*, Application n° 22414/93, § 131.

148. Judgments of 2 December 2009, *European Commission v. Ireland and Others*, C-89/08 P, EU:C:2009:742, § 53; of 4 June 2013, *ZZ v. Secretary of State for the Home Department*, case C-300/11, EU:C:2013:363, § 55. ECtHR, judgment of 19 September 2017, *Regner v. the Czech Republic*, Application n° 35289/11, § 146.

149. *ZZ v. Secretary of State for the Home Department*, cit., § 60. ECtHR, judgments of 19 September 2017, *Regner v. the Czech Republic,* Application n° 35289/11, §§ 152 to 153; 16 February 2000, *Jasper v. the United Kingdom*, Application n° 27052/95, § 56.

150. *ZZ v. Secretary of State for the Home Department*, cit., §§ 57 to 65. *Regner v. the Czech Republic*, cit., § 148; of 29 April 2014, *Ternovskis v. Latvia*, Application n° 33637/02, § 67.

suring that the essence of the right to a fair trial is not compromised[151]. Moreover, the right of individuals cannot be completely emptied: they must, at the very least, be given the substance of the grounds upon which the decision to use surveillance is based[152]. It is however, not self-evident how this case law can be put into practice in the case of spyware. Indeed, as illustrated above, secret surveillance is usually not brought to the knowledge of the individual concerned; moreover, the use of spyware barely leaves traces[153]. That makes it very difficult for individuals to take defensive measures in practice.

According to the Venice Commission, "[g]iven the extraordinary intrusiveness of spyware compared to other surveillance approaches, the screening of authorised and unauthorised (or relevant and irrelevant) information may be difficult as a technical matter. The Venice Commission strongly urges States considering the use of spyware to ensure that it has, as a required safeguard, specialised, vetted, professional teams capable of implementing effective information screening as is required with respect to other information-gathering practices. Destruction requirements [related to unlawfully gathered material] should also be in place, backed up by strong, independent and well-resourced external oversight. This external oversight must be robust and functional both in theory and in practice"[154]. Prof. Ní Aoláin considers in her abovementioned report that if there is no audit record of the spyware activity on a device, the use of spyware is incompatible with human rights law. That is an important finding. At the same time, it has a practical limitation with regard to those instances where spyware is used merely to listen in and not to build evidence[155]. Therefore, it is to be asked whether Member States should not set up, in addition to the independent authority/body provided for in Article 4(8) EMFA, an ombudsman-type of organ with unlimited access to the authorities' surveillance activities. Such an organ would play a complementary and decisive control function, so that there would be an effective check on the use of spyware[156], at least *ex post facto*. Where a State has not established a specialised security oversight body, Data protection Authorities (DPAs) may play an important role in the system of oversight of security and intelligence as a whole[157]. Given the quantity of the data accessed, their sensitive nature and the risk of unlawful access, the data obtained through the use of spyware must be retained in the European Union and must be irreversibly destroyed after the end of the authorization period[158].

Since the common constitutional traditions of the Member States are part of EU law, it is worthwhile to mention some of the rules and constitutional rulings issued by national courts of those States and pertaining to spyware. For example, the German Constitutional Court ruled that public authorities have not only a negative but also a positive obligation to protect fundamental rights from Trojan software attacks against individuals[159]. In a similar vein, the French *Conseil constitutionnel* declared two provisions of a reform of procedural criminal law to be contrary to the French Constitution because they provide for the use of spyware in the pursuit of all kinds of general crimes[160]. Moreover, the law and practice of

151. *Regner v. the Czech Republic*, cit., § 148; ECtHR, judgment of 18 January 2022, *Adomaitis v. Lithuania*, Application n° 14833/18, §§ 68 to 74.

152. See, by analogy, *ZZ v. Secretary of State for the Home Department*, cit., § 65; judgment of 22 September 2022, *GM v. Országos Idegenrendézeti Főigazgatóság*, C-159/21, EU:C:2022:708, § 51.

153. European Data Protection Supervisor 2022, p. 4.

154. Venice Commission 2024, § 85.

155. See, to this effect, *ivi*, § 117.

156. The idea has been given to me by Professor Amnon Reichman in a conversation held at the European University Institute in the autumn of 2024. See to this effect also *ivi*, § 117.

157. *Ivi*, § 118. See also, by analogy, *Tele 2 Sverige and Watson*, cit., § 123.

158. See, by analogy, *Tele 2 Sverige and Watson*, cit., § 122.

159. See above fn. 117.

160. *Decision of 16 November 2023, n° 2023-855 DC*, § 68.

third countries is relevant, given the transnational nature of spyware: for example, in the USA, the authorities included NSO (the Israel-based producer of the notorious spyware "Pegasus") in its Entity List for acting against US national security and foreign policy interests, effectively banning USA companies from supplying NSO. In parallel, litigation is being pursued by some USA tech giants against NSO in the USA: on 9 January 2023, the USA Supreme Court ruled that WhatsApp (belonging to Meta - former Facebook) is allowed to pursue a lawsuit against NSO with regard to the deployment of Pegasus. On 20 December 2024 a federal USA judge ruled that NSO was liable under USA federal and California law for hacking activity that breached over 1,000 WhatsApp users in 2019[161].

In conclusion, whilst spyware is a matter that presents many technical issues, it is, first and foremost, a question of major constitutional importance, raising issues such as: the competences of the Union to regulate the matter (even going beyond EMFA), the compliance with fundamental rights, and the translation of the values under Article 2 TEU into legislation and enforcement action. In this context, legal tensions often arise such as the tension between the constitutional identity of the Union and the constitutional identity of the Member States (e.g., with regard to national security): the reconciliation between both identities is probably one of the most difficult legal challenges that the Union and its Member States will have to face in the near future. The regulation of spyware is one of the most interesting litmus tests for examining the interplay between these constitutional identities[162]. In this context, it should be recalled that, as explained above, EU law, including the protection of fundamental rights (also in light of the ECHR) remains applicable also when national security is invoked.

3. The issue of legal basis: media-specificities and misunderstandings?

This leads to the issue of the legal basis for Article 4 EMFA and for the Act in general. The EMFA is based on Article 114 TFEU, which is the general internal market legal basis in the EU treaties. During the first part of the negotiation process, the issue of the legal basis of EMFA was hotly debated. Political and private entities and Member States which perceived the EMFA as an intolerable intrusion into their political or business autonomy rallied against the legal basis. The ensuing discussion was intense and not always deprived of ideology. Ideally, the debate, in order to be objective, would have relied on a complete picture of the CJEU case law regarding Article 114 TFEU as legal basis and would have engaged with the details of the Commission's impact assessment and with the content of the Commission's proposal for EMFA. It is an open question whether that has always been the case. In any event, a turning point in the debate was the issuance on 4 April 2023 of the Opinion by the Council Legal Service confirming in substance that Article 114 TFEU can be used as legal basis of the EMFA[163].

In the debate, one of the criticisms against the legal basis of the EMFA is that it regulates the cultural and fundamental rights aspects of the media[164]. This criticism, even when expressed in good faith, relies on a misconception both of what internal market legislation does and of the characteristics of the media sector. The Treaty, by establishing a common market and progressively approximating the economic policies of the Member States, seeks to unite national markets into a single market having the characteristics of a domestic market[165]. When regulating the internal market, the legislator pursues the cross-national integration of markets and their "opening up", and at the same time – precisely because it creates new freedom spaces on the market – it also needs to

161. Lyngaas 2024.

162. The idea has been given to me by Alberto De Gregorio Merino in a conversation in the 2023/24 winter at the Legal Service of the European Commission.

163. Opinion 8089/23.

164. See also Cornils 2024 under I, 2. and III.

165. Judgment of 9 February 1982, *Polydor*, Case 270/80, EU:C:1982:43, § 16.

take care of overriding reasons of public interest[166]. To that end, the legislator may, and in fact, must take into account the EU's values and fundamental rights[167]. Even though Article 2 TEU (laying down the values of the EU) and the Charter of fundamental rights of the EU do not establish competences in themselves, they set up requirements for legislation[168]. As the Council Legal Service in its Opinion on the legal basis of EMFA observed, "pluralism is recognised as an essential attribute of society in Article 2 TEU, which sets out the values on which the Union is founded. The Court has ruled on 16 February 2022 on the rule of law conditionality regulation that 'the European Union must be able to defend those values, within the limits of its powers as laid down by the Treaties'. This case law indicates that the Union legislature is empowered to ensure the protection of the values mentioned in Article 2 TEU and of other fundamental rights where it has an appropriate legal basis for taking legislative action"[169].

So, for example, when harmonizing the production and sale of mundane products such as heating system devices in the EU, the legislator not only harmonizes the rules by integrating and opening up the market, but also by taking care of further public interests such as the safety of users, environmental protection, the protection of consumers, and the protection of privacy. This holistic nature of the legislator's action is, as such, neither unlawful nor extraordinary[170]: not unlawful because the legislator is bound to further the values of the EU when disbursing its task, and not extraordinary because socio-economic phenomena cannot be split into purely economic aspects, on the one hand, and other aspects on the other[171]. Such splitting would be artificial and would not reflect the multifacetedness and complexity of reality. This is particularly true for the media, which differs from other products such as heating system devices. Since media are "special goods" and media freedom represents not only a feature of the media service, but also a cornerstone of democracy shaping public opinion and the consequent political decisions, the malfunctioning of the media market might go hand in hand with breaches to the rule of law[172].

What is crucial for the purposes of the legal basis analysis of the EMFA is that the freedom and independence of the media are not only comprised by the fundamental rights protection but also contribute to the quality of the service: as noted above, a media service produced without full editorial freedom and independence lacks quality and thus this aspect is important for the good functioning of the internal market, as it follows from recitals 16 and 17 EMFA. Therefore, economic aspects are not a mere pretense to regulate fundamental rights in the EMFA. The fact that a media service provider is – directly or indirectly, actually or potentially – interfered with in the exercise of its economic activity entails a restriction of its economic rights in the internal market and an uneven playing field. That in turn has repercussions on editorial freedom and independence.

Those who overlook that circumstance fall into the second misconception. Indeed, in order to provide a basis for mutual recognition in the internal market, traded products must fulfill certain basic production standards, such as food safety regulations, as well as other requirements for the protection of consumers[173]. The same applies to media services: as explained, editorial independence and freedom constitute basic quality standards for the media services. Therefore, the regulation of the economic aspects of media necessarily entails at least some regulation of the related fundamen-

166. See, *ex multis,* Judgment of 3 December 2019, *Czech Republic v. European Parliament and Council*, C-482/17, EU:C:2019:1035, § 36.

167. Judgment of 22 January 2013, *Sky Österreich*, C-283/11, EU:C:2013:28, § 51.

168. Judgment of 29 July 2024, *Valančius*, C-119/23, EU:C:2024:653, § 47. See also Bayer 2024, p. 116; Longo 2025, pp. 9-10.

169. Opinion 8089/23, § 55.

170. See also Roß 2023, p. 460.

171. See also Malferrari 2023, pp. 49-50.

172. Brogi–Da Costa Leite Borges–Carlini et al. 2023, p. 38.

173. Bayer 2024, pp. 114-115; Malferrari–Gerhold 2024, pp. 894-895.

tal right aspects, because in the case of the media, they are inextricably intertwined with each other and represent two sides of the same coin[174]. In other words, the value-laden nature of the media sector[175] obliged the legislator to properly take the values and fundamental rights into account when regulating the media services. Indeed, the media market is the marketplace of ideas and opinions, so that regulating that marketplace entails taking into account the freedom of expression and the cultural characteristics of the media. As explained in the Explanatory memorandum accompanying the Commission proposal[176], "[t]he EU legislator must not only comply with fundamental rights when regulating the internal market, but also balance competing fundamental rights. The present Regulation proposal constitutes a harmonious, coordinated and multi-pronged legislative framework by which the legislator contributes to the development and protection of the internal market for media services, thereby also pursuing several further legitimate public interests (including the protection of users) and reconciling in a fair manner the fundamental rights of all the individuals concerned". The Council Legal Service, in its Opinion on the legal basis of EMFA, remarked that "ensuring the quality of media services or protecting media freedom does not as such exclude the use of Article 114 TFEU"; it further explained as follows: "[e]ven though Article 114(3) TFEU does not mention the freedom and pluralism of media – unlike for example a high level of health protection, environmental protection or consumer protection – it is inherent in the harmonisation under Article 114 TFEU that national rules are harmonised which are taken in the pursuit of specific policies. It is therefore inherent in the logic of Article 114 TFEU that the Union rules harmonising these national rules will relate to these policies. Protecting the freedom of the media and the quality of media services can thus be an essential public interest objective in a legislative act based on Article 114 TFEU if the conditions set out therein are fulfilled"[177]. In light of the foregoing, the legislator in the EMFA cannot be validly criticized for having taken into account the cultural diversity and pluralism of the media when regulating the media services market.

That does, of course, not mean that the conditions for using Article 114 TFEU as the legal basis can be neglected: such conditions must be verified (see more in detail below). But it means that the EMFA cannot be validly criticized for having prominently taken the values fundamental rights into account when regulating the media services: an impact on them is inherent in the nature of the media services. By the same token, an indirect impact on the cultural aspects of the media services cannot be avoided in the case of EMFA precisely because media services have an inherent cultural dimension. Such an impact is, as such, not unlawful and is even implied by Article 167 TFEU, whereby the legislator is to take account of the cultural aspects when using legal bases provided for in the Treaties (such as Article 114 TFEU).

Having made these clarifications, I now examine whether the conditions for using Article 114 TFEU are fulfilled in the case of the EMFA. Since the present essay is concentrated on Article 4 EMFA, I will limit the analysis to that provision. As is well known, Article 114 TFEU, in essence, requires that: i) there is actual or likely regulatory fragmentation; ii) the fragmentation leads to restrictions to the fundamental freedoms or to an uneven playing field, to the detriment of the good functioning of the internal market, iii) the internal market problem is solved through the envisaged EU harmonization[178].

In the case of Article 4 EMFA, first, the State's interferences in or influencing of the editorial policies and editorial decisions of media service

174. Roß 2023, p. 459. See also, to this effect, Vīķe-Freiberga–Däubler-Gmelin–Hammersley–Poiares Pessoa Maduro 2013, p. 20.

175. Council conclusions on safeguarding a free and pluralistic media system (2020), § 18.

176. COM(2022) 457, p. 8.

177. Opinion 8089/23, § 54. See, to this effect, *Sky Österreich*, cit., § 52, and judgment of 3 February 2021, *Fussl*, C-555/19, EU:C:2021:89, §§ 54-55 and case law cited therein. See also Vidal Marti 2023.

178. See, *ex multis,* Judgment of 12 December 2006, *Germany v. European Parliament and Council* (Tobacco Advertising II), C-380/03, EU:C:2006:772, §§ 36 et seq.

providers constitute restrictions to the free exercise of the media service activities in the internal market because the quality of media services requires freedom in the making of the media products: like an industrial product requires the respect for safety standards and a medical service requires the autonomy of diagnosis by the medical professionals, the media service requires the autonomy of the media service providers from the State. Since the media services are increasingly liable to be produced or consumed cross-border[179], a cross-border element is typically present at least in many scenarios[180]. In that regard, recourse to the legal basis of Article 114 TFEU does not presuppose the existence of an actual link with freedom of movement between Member States in each of the situations referred to by the act founded on such a basis. What is important, in order to justify recourse to that legal basis, is that the act adopted on that basis actually has as its object the improvement of the conditions for the establishment and functioning of the internal market. As regards journalistic sources and confidential information related to or capable of identifying journalistic sources, they constitute the "raw material" of the media services, so that their disclosure entails losing their economic value and function for the media service providers, to the detriment of the exercise of the media service activities (see recital 19 EMFA). The same reasoning applies to the detainment, sanctioning, interception and inspections of media service providers or their editorial staff: if the service provider is impaired in its function, a restriction to the exercise of its economic activity is present. The same goes for the deployment of spyware.

Second, the rules protecting editorial independence and journalistic sources are heterogenous across the internal market (recitals 18 and 23 EMFA and Commission's Impact Assessment, pages 8-9)[181]. In particular, in some countries, the data protected by the secrecy of a journalistic sources cannot be collected or analyzed, whereas in other countries, the limits are very different[182]. This finding has been reaffirmed by the Venice Commission as regards spyware[183]. Furthermore, the application of the divergent rules gives rise to legal uncertainty, to the detriment of the good functioning of the internal market[184]. As stated in recital 24 EMFA, "(m)edia professionals, in particular journalists and other media professionals involved in editorial activities, work increasingly on cross-border projects and provide their services to cross-border audiences and, by extension, to media service providers. As a result, media service providers are likely to face barriers, legal uncertainty and uneven conditions of competition. Therefore, the protection of journalistic sources and confidential communications requires harmonisation and further strengthening at Union level". This internal market problem for media service providers is solved by Article 4 EMFA because it opens up the market and lays down a common (minimum) protection for media service providers. It cannot, thus, be validly argued that the EMFA merely has positive side effects for the internal market[185].

It follows from the foregoing considerations that the requirements for the use of Article 114 are fulfilled as regards Article 4 EMFA.

The fact that the legislator limited itself to principled rules and to minimum protection testifies to the respect for subsidiarity and proportionality. In particular, the subsidiarity condition is fulfilled because in the Member States, political forces were

179. Longo 2025, p. 9.

180. See, to that effect, judgments of 20 May 2003, *Österreichischer Rundfunk*, C-465/00, EU:C:2003:294, § 41; of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, § 40.

181. Parcu–Brogi–Verza et al. 2022, pp. IV, 188, 326-327, 351, 366.

182. Venice Commission 2024, § 42.

183. *Ivi*, §§ 37 et seq. (see in particular 61).

184. Cf. *ivi*, § 82: "[w]hile some domestic legal regimes are quite detailed and precise, some others tend to rely on relatively broad and open-ended formulations which do not necessarily provide the required degree of certainty and precision".

185. See, to that effect, Longo 2025, p. 10; Mastroianni 2022, p. 107. But for a different view see Kraetzig 2023, p. 1; Cornils 2024, under III. 3. a).

unwilling to modify the regulatory framework that facilitated or created the market failures that affect the European media market[186]. The choice of a regulation instead of a directive is justified when considering the need for rapid regulation of the digital market[187].

A criticism raised against Article 114 TFEU as the legal basis for Article 4 EMFA is that it violates the Member States' competence for criminal law[188]. This criticism is unfounded. Indeed, Article 4 TFEU does not directly harmonize national criminal law: see also recital 22 EMFA, *in fine*, whereby "[i]t is not the purpose of this Regulation to harmonise the concepts of 'detain', 'inspect', 'search and seizure' or 'surveillance'". Article 4 EMFA rather creates a frame ("encadrement") within which Member States must exercise their competences, be they of an administrative, criminal or private law nature (provided of course that the limits set by Article 114 TFEU are complied with). In that regard, Article 4 EMFA is similar to the Directive on personal data, the e-privacy Directive, and the Regulation on the free flow of non-personal data, which are also based on Article 114 TFEU[189]. The Union's competence to harmonize national law pursuant to Article 114 TFEU is a functional competence; it is not thematically limited, and applies to any measure that affects the establishment or functioning of the internal market[190].

In conclusion, given its novelty, it is understandable that the EMFA raises an issue of legal basis. However, in light of the well-established case law of the CJEU, the examination of the articles of the EMFA, its recitals, the Explanatory Memorandum and the Impact Assessment of the Commission offer more than a sufficient and solid ground for considering Article 114 TFEU as a lawful legal basis. That issue will be adjudicated by the CJEU because Hungary has lodged an annulment action against EMFA as regards the legal basis; the case is pending at the time of writing[191].

4. The future prospects of enforcement of Article 4 EMFA

Article 4(1) and (2) EMFA are applicable since 8 February 2025, whereas the rest of Article 4 EMFA will be applicable from 8 August 2025[192]. A number of issues related to the application of Article 4 EMFA are to be considered at this stage. First, how can it be ensured that the guarantees laid down in Article 4(4) and (5) EMFA are rendered effective in practice? The secrecy of surveillance measures is to be respected (at least to a certain extent) so that at least in many cases, both the authorization of surveillance measures and their execution are carried out without the individual's knowledge. On the other hand, the *effet utile* of Article 4 EMFA requires that measures are taken such as to avoid the guarantees becoming nugatory. In this regard, Article 4(8) EMFA, in its second part, is pertinent. Under this provision, Member States shall entrust an independent authority or body with relevant expertise to provide assistance, with regard to the exercise of the right to effective judicial protection, to media service providers, their editorial staff and any persons who, because of their regular or professional relationship with a media service provider or its editorial staff, might have information related to or capable of identifying journalistic sources or confidential communications. Candidates for being the independent authority or body referred to in this provision could be the data protection

186. Bayer 2024, p. 113.

187. Longo 2025, p. 9.

188. Cf. Ferreau 2024, p. 43.

189. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

190. Schütze 2014, a p. 228.

191. *Hungary v. European Parliament and Council*, C-486/24.

192. Article 29 EMFA.

representative, but it could also be an *ad hoc* authority or even a private entity such as a media service provider chamber or journalist association. An important role to be played by this independent authority or body is to supervise the authorization and the execution of surveillance measures (including verifying the duration and ensuring that the conditions are still being met). The need for the abovementioned independent authority or body is indirectly underpinned by the Venice Commission, which recognized that the absence of information for the target of surveillance measures can, to some extent, be compensated by the presence, in the procedure, of bodies acting as "privacy advocates", i.e., legal professionals that represent the interests of targeted persons and organizations in the authorization procedure[193].

Strict confidentiality obligations can be imposed on the privacy advocates. A security screened advocate does not directly act for the suspect and cannot, obviously, consult with him or her. The advocate may, in practice, be given only a very short time to familiarize with the particulars of the case, and thus be at a procedural disadvantage compared to the requesting authority; on the other hand, the mechanism can still have some value insofar as it can lead to conditions being imposed to minimize the intrusion into privacy, either for the target, or others affected by the surveillance[194]. Moreover, it can formalize the process of obtaining authorization, making it clearer that it is the requesting authority which has the burden of showing the need for the use of surveillance, and that all the conditions for surveillance need to be fulfilled[195].

Second, the media service provider target of surveillance still needs to be notified *ex post facto*, so that he/she can exercise his/her right to judicial remedies, including review and damages actions. During the exercise of that right, there are practical issues that are thorny: are there limits to the scope of the judicial review that arise from the confidentiality of national or public security reasons? It is conceivable that certain documents must be redacted or made entirely confidential; this, however, does not rule out the effective review by a judge, who can handle confidentially reports or other documents (in their entirety or partially redacted). Furthermore, there are doubts about the adequacy of the safeguards where the applicant's presumed situation is such that the information on the authorization of covert information gathering remains confidential and therefore inaccessible to the person concerned[196]. There are some, at least, partial solutions that can be envisaged. For example, a complaint mechanism can be set up to make the review effective; access to classified information can be given to remedial bodies[197]. Furthermore, the use of in-camera proceedings may also provide a practical solution. In addition, the independent authority or body referred to in Article 4(8) EMFA could also be given access to confidential information, on the basis of which it could react in the interest of the individual concerned. According to settled case-law, "the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law; thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[198].

A third issue regarding the application of the provision is whether a judge who has to decide on the prior authorization under Article 4(4)(d) EMFA may pose a preliminary question to the CJEU. As is well-known, one of the conditions for the admissibility of a preliminary reference is that a legal dispute is pending before the referring

193. Venice Commission 2024, § 113.

194. *Ibidem*.

195. *Ibidem*.

196. *Klaudia Csikós v. Hungary*, cit., § 66.

197. European Union Agency for Fundamental Rights 2023; Venice Commission 2024, § 123.

198. Judgment of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, § 187.

judge[199]. In the present scenario, there is, at least nominally, a counterpart which is the person who is to be subjected to surveillance ("the target"). The fact that this person is excluded from the procedure on the ground of the confidentiality of the investigation does not make the adversarial nature of the procedure evaporate. There is, on the merits of the case, a dispute before the authorizing judge, who would thus be empowered to refer a question of interpretation and/or validity to the CJEU under Article 267 TFEU[200]. The reference however should be drafted in such a way that several details are made confidential, in order to avoid the risk that the individual recognizes his/her situation and thus becomes aware in advance of the fact of being subject or being liable to be subject to surveillance.

A fourth issue concerns the role to be played by the media regulators and the Board (which consists of the national regulators pursuant to Article 10(1) EMFA). In the first place, the Board, upon the Commission's request, is to draft opinions on technical and factual issues related to Art. 4(4)(c)[201]. The Board's decisions are taken with a 2/3 majority. Whereas these opinions are by definition not binding, they carry some weight in the assessment to be made by national authorities, which must take them into account on the ground of loyal cooperation under Article 4(3) TEU. According to recital 41, the Board's opinions "should serve as useful guidance for the national regulatory authorities or bodies concerned and could be taken into account by the Commission in its tasks of ensuring the consistent and effective application of this Regulation and the implementation of Directive 2010/13/EU. By making their best effort to implement the opinion of the Board or by properly explaining any deviation therefrom, national regulatory authorities or bodies should be considered to have done their utmost to take the opinion of the Board into account". In the second place, the Board shall, inter alia, "promote cooperation and the effective exchange of information, experience and best practices between the national regulatory authorities or bodies on the application of (…) this regulation"[202]. The Board shall foster the exchange of best practices among the national regulatory authorities or bodies, consulting stakeholders where appropriate, on regulatory, technical or practical aspects relevant to the consistent and effective application of this Chapter of the EMFA and the implementation of AVMSD[203].

A fifth and final issue concerns the role to be played by professional associations, in particular journalist associations. Their role is not prominently provided for in EMFA. There is reference to "other relevant bodies and sources" made in Article 27(4)(a) EMFA in the context of the evaluation and reporting to be carried out by 8 August 2028. According to recital 40, "[w]here the Board deals with matters beyond the audiovisual media sector, it should rely on an effective consultation mechanism involving stakeholders from the relevant media sectors active both at Union and national level. Such stakeholders could include press councils, journalistic associations, trade unions and business associations. The Board should give such stakeholders the possibility to draw its attention to the developments and issues relevant to their sectors. The consultation mechanism should enable the Board to gather targeted input from the relevant stakeholders and obtain relevant information supporting its work. When establishing the arrangements for the consultation mechanism in its rules of procedure, the Board should take into account the need for transparency, diversity and fair geographical representation. The Board should also be able to consult academia in order to gather additional relevant information". Going beyond this, professional associations may play a decisive role in providing input to further institutional actors, in bringing collective actions via national

199. See, *ex multis,* Order of 18 June 1980, *Borker*, Case 138/80, EU:C:1980:162, § 4.

200. See, to this effect, *Procura di Bolzano*, cit., which concerned the request for authorisation from a judge in order to access personal data retained by providers of electronic communications services, with a view to the prosecution of crimes.

201. Article 13(1)(c)) EMFA.

202. Article 13(1)(b) EMFA.

203. Article 16(1) EMFA.

procedural law channels and in assisting media service providers on legal and technical matters.

5. Conclusion

The internal market cannot be confined to a purely welfare-maximizing project. Whereas the values enshrined in Article 2 TEU are formulated in broad terms, they have a legal significance that must be preserved and propagated (cf. Article 3 TEU)[204]. Public powers in the EU are bound to pursue the values shared by the EU and its Member States. A common EU media policy that would better concretize the European values is an indispensable precondition for the European integration project especially considering the deepening of the geopolitical crisis[205]. Indeed, the media have been under attack in the Union in several ways. Political forces and national governments often perceive free media as a nuisance at best and otherwise as a tool to be domesticated and used for their purposes; in the worst case, free media are even considered to be a hindrance that must be gotten rid of. Furthermore, social media and non-journalistic content have been increasingly consumed by citizens and undertakings in lieu of proper media services[206]. Truth is a rare and expensive commodity[207]. Disinformation and AI-produced content are certainly cheaper to produce and easier to get the favor of algorithms, which aim at maximizing users' engagement and thus gives disproportionate resonance to polarizing or radical content. Thus, quality media services risk remaining squeezed in the digital and AI era. In addition, risks to the EU's internal media market from third countries are increasing: for ex., foreign misinformation is systematically used as a "weapon"[208].

Against this dire backdrop, the need for a liberal legal protection of the media services at European level can barely be called into question. Since for the media the challenges related to the market and the values are increasingly cross-border and the hindrances stem from national actors (mainly governmental ones), it was for the EU to step in and act. Obviously, the EMFA is not a panacea for the many arduous challenges affecting the media services in the internal market. But, albeit minimalist, the EMFA tries to address these challenges. In particular, it safeguards the rights of media service providers, including journalists, and protects their independence in many regards; by doing so, the EMFA not only develops the internal market further, but it also paves the way for a more resilient and democratic European Union[209]. The obligation of effective editorial freedom and independence of media service providers and the prohibition to interfere in or try to influence their editorial policies and editorial decisions give more precision to existing obligations under the Charter and the ECHR. The relevance of Art. 4 (3-9) EMFA consists in particular in creating a supranational level of normativity and an additional layer of control of implementation which is important because there is limited compliance in several Member States with the ECtHR's case law on Article 10 ECHR. The tandem of the national judiciary as *juge commun du droit européen* and the CJEU as well as the Commission through the infringement procedure offer enforcement possibilities which the ECHR does not possess.

The internal market is a living instrument[210]. The EMFA can be considered to be an impressive example of the vitality and dynamism of the Union legislation as instrument of policy making[211]. The EMFA develops the internal market law in light of the fundamental rights laid down in the Charter of fundamental Rights, by strengthening existing guarantees and enabling a vibrant economic sector to regain thrust and to develop further, including

204. See AG Ćapeta Opinion in *Commission v Hungary* ("anti-LGBTQ"), C-769/22, EU:C:2025:408, § 155 et seq.

205. Bayer 2024, p. 109.

206. Newman 2024.

207. Harari 2024, p. 17.

208. Article 17 EMFA aims at tackling this problem in particular. See Malferrari 2023, pp. 49-50.

209. Verheyen 2024.

210. See, to this effect, Opinion of AG M. Szpunar of 18 May 2017, *Visser*, Joined Cases C-360/15 and C-31/16, EU:C:2017:397, § 2.

211. Cf. Cornils 2024, VI.

across borders[212]. The economic aspect of the media and their value-laden nature constitute two sides of the same coin they are merged with each other in the EMFA. There is harmony between the EU's economic efficiency (in particular through the opening of the markets and free competition) and its values, because the reconciliation of all those public objectives is the cement that keeps individuals and society together in a regionally, culturally and socially diverse and sometimes divergent Europe[213]. Thus, the EMFA also contributes to the development of a European society, which is an immensely valuable resource for current and future generations.

References

J. Bayer (2024), *Digital Media Regulation within the European Union. A Framework for a New Media Order*, Nomos, 2024

E. Brogi, D. Da Costa Leite Borges, R. Carlini et al. (2023), *The European Media Freedom Act: media freedom, freedom of expression and pluralism*, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, Study PE 747.930, 2023

M. Cole, C. Etteldorf (2024), *The European Media Freedom Act unpacked*, European Audiovisual Observatory, 2024

M. Cole, C. Etteldorf (2023), *European Media Freedom Act – Background Analysis*, European Parliament Policy Department for Structural and Cohesion Policies, Directorate-General for Internal Policies, PE 733.129, 2023

M. Cornils (2024), *Der Funktionsschutz der Medien als Aufgabe des Unionsrechts*, in "Zeitschrift für Gesetzgebung", vol. 39, 2024, n. 4

European Union Agency for Fundamental Rights (2023), *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU*, 2023

European Court of Human Rights (2022), *Guide on Article 10 of the European Convention on Human Rights – Freedom of expression*, 2022

European Data Protection Supervisor (2022), *Preliminary Remarks on Modern Spyware*, 15 February 2022

J.F. Ferreau (2024), *Rechte von Mediendienstanbietern (Art. 4)*, in Id. (ed.), "Das neue EU-Medienfreiheitsgesetz", Nomos, 2024

L. Gerhardinger (2023), *Journalistischer Quellenschutz im Zeitalter der Digitalisierung und Globalisierung*, Mohr Siebeck, 2023

O. Grandinetti (2024), *Quale nozione di pluralismo nell'EMFA?*, in "Rivista italiana di informatica e diritto", 2024, n. 2

Y.N. Harari (2024), *Nexus. A Brief History of Information Networks from the Stone Age to AI,* Random House, 2024

K. Jakubowicz (2015), *New Media Ecology: Reconceptualizing Media Pluralism*, in P. Valcke, M. Süksöd, R.G. Picard (eds.), "Media Pluralism and Diversity", Palgrave Macmillan, 2015

J.E. Kermer (2024), *Article 4 of the European Media Freedom Act: A Missed Opportunity? Assessing Its Shortcomings in Protecting Journalistic Sources*, in K. Simeonov, M. Yurukova (eds.), "The Agenda of

212. See also Paolucci 2024.

213. See Triantafyllou–Malferrari 2022, p. 330. Cf. also von Bogdandy 2024, pp. 11-13.

the New EU Institutional Cycle. Papers from the Eleventh International Scientific Conference of the European Studies Department", Sofia University, 2024

J.E. Kermer (2024-a), *How far does Article 4 of the European Media Freedom Act go in banning state surveillance of journalists?*, Centre for Media Pluralism and Media Freedom, 26 November 2024

V. Kraetzig (2023), *Freedom Governed by Brussels*, in "Verfassungsblog: On Matters Constitutional", 12 June 2023

E. Longo (2025), *Grounding media freedom in the EU: The legal basis of the EMFA*, in "Rivista italiana di informatica e diritto", 2025, n. 1

S. Lyngaas (2024), *Judge rules Israeli firm NSO Group liable for damages in WhatsApp hacking case*, CNN, 20 December 2024

L. Malferrari (2023), *Der European Media Freedom Act als intra-vires-Rechtsakt*, in "Europäische Zeitschrift für Wirtschaftsrecht", vol. 34, 2023, n. 49

L. Malferrari, M. Gerhold (2024), *Ein Unionsrecht auf Empfang pluraler Medien?*, in "Europäische Zeitschrift für Wirtschaftsrecht", vol. 35, 2024, n. 19

R. Mastroianni (2022), *Freedom and pluralism of the media: an European value waiting to be discovered?*, in "MediaLaws", 2022, n. 1

H. Mildebrath (2022), *Europe's PegasusGate. Countering spyware abuse*, European Parliamentary Research Service, 2022

N. Newman (2024), *What do we Know about the Rise of Alternative Voices and News Influencers in Social and Video Networks?*, Digital News Report 2024 sec. 2.5, Reuters Institute and University of Oxford, 2024

F. Ní Aoláin (2023), *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism – Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, UN Human Rights Council, 2023

F. Palmiotto (2024), *Criminal investigations, access to data and fundamental rights: The role of judicial review after Procura*, in "Common Market Law Review", vol. 61, 2024, n. 6

F. Paolucci (2024), *The European Media Freedom Act: (another) new chapter in the digital regulation saga*, in "Diritti Comparati", 6 May 2024

P.L. Parcu, E. Brogi, S. Verza et al. (2022), *Study on media plurality and diversity online*, Publications Office of the European Union, 2022

R. Phillips (2023), *The Efficacy of European Union Spyware Regulations*, in "Student Occasional Paper", Tech4Humanity Lab, 2023, n. 5

H. Raab (2022), *Wie wir die Freiheit der Medien bewahren*, in "Frankfurter Allgemeine Zeitung", 30 July 2022

Reuters (2025), *Italian government under pressure in Paragon spyware row*, 7 February 2025

Reuters (2024), *Digital News Report 2024*

L. Roß (2023), *European Media Freedom Act und Kernfragen der europäischen Integration*, in "Europarecht", vol. 58, 2023, n. 5

R. Schütze (2014), *Limits to the Union's 'Internal Market' Competence(s): Constitutional Comparisons*, in L. Azoulai (ed.), "The Question of competence in the European Union", Oxford University Press, 2014

M. Trevisan, V. Štětka, M. Milosavljevič (2024), *Tools and strategies of political capture of the media in Europe*, in E. Brogi, I. Nenadić, P.L. Parcu (eds.), "Media Pluralism in the Digital Era", Routledge, 2024

D. Triantafyllou, L. Malferrari (2022), *The European Commission: the clock master of the European Union Internal Market*, in European Commission (ed.), "70 Years of EU law – A Union for its citizens", Publications Office of the European Union, 2022

P. Valcke, R.G. Picard, C. Dal Zotto (2015), *Indicators for Media Pluralism*, in P. Valcke, M. Süksöd, R.G. Picard (eds.), "Media Pluralism and Diversity", Palgrave Macmillan, 2015

Venice Commission (2024), *Report on a rule of law and human rights compliant regulation of spyware*, CDL-AD(2024)043, 13 December 2024

S. Verheyen (2024), *Der Europäische Medienfreiheitsakt: Ein Meilenstein für die Pressefreiheit in der EU*, in "Europäische Zeitschrift für Wirtschaftsrecht", vol. 35, 2024, n. 12

S. Verza (2025), *What is journalism in the digital age? Key definitions in the European Media Freedom Act*, in "Rivista Italiana di informatica e diritto", 2025, n. 1

N. Vidal Marti (2023), *The Key to Ensure Media Pluralism in the EU? A Unified Framework*, in "Verfassungsblog: On Matters Constitutional", 12 June 2023

V. Vīķe-Freiberga, H. Däubler-Gmelin, B. Hammersley, L.M. Poiares Pessoa Maduro (2013), *A free and pluralistic media to sustain European democracy*, European Commission, 2013

A. von Bogdandy (2024), *On the Meaning and Promise of European Society*, in "MPIL Research Paper Series n. 2024-30", 2024

D. Voorhoof (2025), *European Court of Human Rights: Klaudia Csikós v. Hungary*, European Audiovisual Observatory, 2025

D. Voorhoof (2022), *European Media Freedom Act and the protection of journalistic sources: still some way to go*, 18 November 2022

D. Voorhoof (2021), *Case Law, Strasbourg: Big Brother Watch v. United Kingdom, Bulk interception regime violated Articles 8 and 10*, 9 June 2021

S. Woodhams (2021), *Spyware: An unregulated and Escalating Threat to Independent Media*, Centre for International Media Assistance (CIMA), 25 August 2021