ARTICLE 4 OF THE EUROPEAN MEDIA FREEDOM ACT: A MISSED OPPORTUNITY? ASSESSING ITS SHORTCOMINGS IN PROTECTING JOURNALISTIC SOURCES

Research Associate Jan Erik Kermer, PhD
Centre of Media Pluralism and Media Freedom

Abstract

Article 4 of the recently approved European Media Freedom Act (EMFA) aims, first and foremost, to protect journalists as well as safeguarding their sources by prohibiting or at the very least limiting the use of state surveillance technology. Despite its apparently good intentions, there are several potential loopholes and shortcomings of this Article which are laid out in this paper. To begin with, Article 4 essentially legalises the use of spyware in EU law, albeit under exceptional circumstances. In addition, the provision permitting the retrospective authorisation of spyware opens up the possibility of journalists' rights being violated before the intervention of the law. The Article, furthermore, affords too much discretion for EU governments to deploy spyware. To compound matters, expanding the list of „serious crimes" to offences such as intellectual property theft and piracy is disproportionate when weighed against the fundamental rights at stake. The scope, moreover, includes crimes carrying a custodial sentence of 5 years, as defined solely under national law, thus undermining the original purpose of EMFA, which is to harmonise national regulatory systems related to the media. Most concerning, however, is the loophole in this Article which fails to outlaw surveillance outsourcing to private entities. In sum, EMFA affords too much discretion for states to deploy draconian surveillance measures that ultimately threaten journalistic sources. To conclude, recommendations are elaborated to overcome the limitations and risks previously analysed.

Keywords: EMFA, Article 4, Surveillance, Spyware, Journalism, Sources, Safety

Introduction

Journalists are and continue to be one of the primary targets of repressive state surveillance measures (Freedom House, 2023; Bleyer-Simon et al., 2024). In the fulfilment of their crucial accountability and watchdog function, journalists are expected to investigate any wrongdoing or corruption in government, making

them highly vulnerable to the prying eyes of the state. In addition, journalists might frame the news in ways that challenge politicians' core narratives or report stories which undermine support for the ruling party. As a result, governments – while they would be reluctant to admit it – are resorting to drastic surveillance measures as part of a concerted effort to stifle criticism, promote self-censorship, ensuring that journalists 'toe the party line.' Countless numbers of journalists from around the world have been subjected to intrusive state surveillance. Jamal Khashoggi (Saudi Arabia), Javier Valdez Cárdenas (Mexico), Omar Radi (Morocco) and Maati Monjib (Morocco) are widely cited examples (see Woodhams, 2021, pp. 8-10 for a detailed summary on each case). While this maligned practice appears more widespread in third countries, many cases have been reported in Europe, as well[1]. One famous example is the case of a Greek journalist, Thanasis Koukakis, in 2021, who was allegedly targeted with Predator spyware by the Greek state agency, the National Intelligence Service (EYP). Worryingly, this phenomenon shows no signs of abating, with several cases reported in 2023, most notably, Alesya Marokhovskaya and Irina Dolinina Alesya Marokhovskaya, two Prague-based Russian journalists who were allegedly subjected to surveillance from Russian state agencies (Committee to Protect Journalists, 2023). In the same year, the Russian independent media outlet, *Meduza* (Latvia) had allegedly been affected with Pegasus software, although the perpetrator has not yet been identified (Access Now, 2023).

The findings from recent implementations of the Media Pluralism Monitor (MPM, 2022-24) repeatedly show that spyware is being used by several member states to snoop on journalists, particularly in Hungary (Bátorfy et al., 2022) but also in Latvia (Rožukalne and Skulte, 2024) and the Czech Republic (Štětka et al., 2024). According to the Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation), the abuse of human rights through the surveillance of „journalists, politicians, law enforcement officials, diplomats, lawyers, businesspeople, civil society actors, and other actors" using Pegasus and equivalent software is widespread throughout the whole EU (Phillips, 2023:3). The PEGA committee even suspects that „all Member States have purchased or used one or more spyware systems" (Veld, 2023). These findings are corroborated by Amnesty International's so-called „Predator files" (2023), concluding that the EU had failed to adequately regulate spyware and uphold human rights standards, as well (Phillips, 2023:2). The same report highlights the deleterious effects of preexisting EU legislation and the lack of risk evaluation and government oversight, despite export regulations, when distributing these technologies, thus posing a threat to people's fundamental rights in general and journalistic sources in particular (Phillips, 2023:3). According to one scholar, cybersecurity companies are exploiting the regulatory fragmentation in the EU and the countries with lax legal protections particularly in Cyprus, Bulgaria, Greece (Feldstein et al., 2023).

[1] As has been well-documented by several high-profile reports, such as the PEGA committee investigations, the deployment of spyware is widespread across Europe.

Noting these issues, the European Media Freedom Act is a timely and unprecedented piece of EU regulation which seeks to strengthen the pluralism and independence of the media within the European Union[2]. The Act aims, inter-alia, to ensure transparency of media ownership, prevent political interference in editorial decisions, protect journalists by safeguarding their sources and prohibiting the use of spyware against them, defend online media content from unjustified removal, establish a new European board for media services, and set standards for audience measurement systems and promote the transparent allocation of state advertising (Brogi et al., 2023). Following months of negotiations, in January 2024, the trilogue compromise text was approved by the Permanent Representatives' Committee and confirmed by a vote in the Committee on Culture and Education. On 13 March, the European Parliament voted on the agreement. On 26 March, EMFA received its final approval from the Council (Centre of Media Pluralism and Media Freedom, 2024).

In essence, the central aim of Article 4 is to protect journalistic sources[3] by prohibiting or restricting, as much as possible, the deployment of intrusive surveillance tools on journalists (Brogi et al.,2023). Article 4 is the EU's response to the increasing usage of sophisticated spyware technologies, which have strengthened the state's capacity for intelligence gathering and surveillance. Spyware technology can be understood as Janus-faced; on the one hand, this technology arguably enhances the state's ability to combat terrorism and criminal activity, on the other hand, it risks undermining people's privacy in general and the confidentiality of journalists' sources in particular (Brogi et al.,2023:48).

To summarise the main provisions in more detail, Article 4 of the European Media Freedom Act (EMFA) aims to safeguard journalistic sources by prohibiting the use of state surveillance upon journalists, save for rare and exceptional circumstances[4]. Article 4(1) grants media service providers (hereafter referred to as MSPs) the right to conduct economic activities in the internal market freely, save for those allowed under Union law, as per Article 4 para.1. Member States are prohibited from interfering with MSPs' editorial policies, and decisions (Article 4 para.2). Paragraph 3 obliges Member States to protect journalistic sources and confidential communication. However, this appears to be a rather vague and hollow commitment, especially considering the numerous derogations granted and loopholes introduced under this provision. Paragraphs 3a-c set out the kinds of surveillance activities which are prohibited. Member States cannot:

---

[2] This paper builds on the Centre of Media Pluralism and Media Freedom's study, in particular the section on Article 4 requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) titled: „The European Media Freedom Act: media freedom, freedom of expression and pluralism" (Brogi, Borges, Bleyer-Simon, Carlini, Nenadic, Kermer, Reviglio, Trevisan, Verza, 2023).

[3] The protection of journalistic sources overlaps with values enshrined in the Charter of Fundamental Rights of the European Union (CFREU) in particular, personal data protection (Article 8 CFREU) and the freedom of expression (Article 10 CFREU).

[4] Article 4 seeks to safeguard editorial freedoms and independence, unless it complies with Article 52(1) of the Charter of the European Union and other Union law.

oblige MSPs to disclose information capable of identifying journalistic sources (referred to hereafter as the „forced disclosure" provision); detain, sanction, intercept, surveil or search MSPs (referred to hereafter as the „detain-and-intercept" provision) or deploy „intrusive surveillance software" on the devices of MSPs (the so-called „anti-spyware" provision). Paragraph 4 contains lays out the specific circumstances under which state surveillance measures may be allowed (the so-called „derogation provisions"). Significantly, it is worth noting that ex-ante judicial protection has been included in the final agreed text, meaning that state surveillance measures authorised by judicial bodies are permitted. Moreover, surveillance measures may be authorised for the investigation of offences listed in Article 2(2) of Framework Decision 2002/584/JHA or for „serious crimes" as determined by the law of a Member State. Paragraph 6 ensures that state surveillance measures are subject to a regular review by a judicial authority to determine whether the conditions justifying their use continue to be fulfilled. Paragraph 7 invokes Directive (EU) 2016/680 (the so-called „Law Enforcement Directive") which regulates the processing of personal data by law enforcement authorities. Paragraph 8 invokes Article 47 CFR, which guarantees the right to an effective remedy and a fair trial, and finally, Paragraph 9 ensures that the obligations placed on Member States under the Treaty on the Functioning of the European Union (TFEU) and the Treaty on European Union (TEU) are respected. Article 4 builds on several EU directives, Council of Europe conventions and European Court of Human Rights (ECHR) jurisprudence which tangentially strengthen source protection to different extents and with varying degrees of success (Brogi et al.,2023:49).

Before embarking on critically examining Article 4 of EMFA, it is important to place the legal treatment of spyware in a historical context to gain a richer understanding of how spyware was regulated in the past. The protection of journalistic sources can be traced back to 1981 with the ratification of the Council of Europe's „Convention 108" (Council of Europe, 2016a). While the Convention did not explicitly address journalistic sources, it established, for the first time, a legal framework for personal data protection. The overarching aim of this Convention was to protect individuals against potential abuses during the collection and processing of personal data. Moreover, the Convention, as per Article 12, outlawed Member States from limiting the transborder flow of personal data which indirectly helped foster cross-border flows of information (Brogi et al.,2023:49). Whilst the Convention aimed to protect personal data from unauthorised access, as per Article 7 of the Convention, certain derogations were established such as those pertaining to state security interests (Brogi et al.,2023:49). The Privacy and Electronic Communications Directive 2002/58/EC established a legal precedent in protecting the privacy in the handling of personal data in electronic communications, however, it did not specifically address journalistic sources. The Directive, nonetheless, included provisions which contributed indirectly to safeguarding the confidentiality of sources, in particular, Article 5(1) which prohibited the „listening, tapping, storage or other kinds of interception or surveillance of communications [...] without the consent

of the users concerned". As with the Convention, certain derogations were introduced such as supporting criminal investigations and national security concerns (see, for instance, Article 15). In 2016, the EU adopted the General Data Protection Regulation (GDPR) requiring media service providers to implement appropriate safeguards in maintaining the confidentiality of journalistic sources. While the GDPR introduced measures to safeguard personal data, as per Recital 153, journalists have been granted several exemptions subject to a balancing test that weighs the overall public interest against individual rights and freedoms (Brogi et al.,2023:49). In 2019, the Whistleblower Protection Directive (2019/1937) came into force to further protect journalistic sources (see Recital 46 in particular). More recently, the European Commission has adopted Recommendation (C/2021/6650) „on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union", which is an important component of source protection. Therein, the issue of surveillance against journalists was acknowledged, however, recommendations are, by definition, not legally enforceable so its potential impact in practice is questionable. More significantly, in April 2024, the Council of the European Union adopted the „anti-SLAPP" Directive (EU) 2024/1069, which is expected to help thaw the chilling effect of strategic lawsuits against public participation (SLAPPs) on the free circulation of information.

Two laws in particular can be regarded as precursors to Article 4 on regulating spyware: (1) Regulation (EU) 2021/821 of the European Parliament (EUDUR) and of the Council of 20 May 2021, and (2) the Wassenaar Arrangement (WA). The former established a comprehensive Union regime for controlling the export, brokering, technical assistance, transit, and transfer of dual-use items, which include goods, software, and technology, used for both civilian and military purposes (Akin Gump Strauss Hauer & Feld LLP, 2021). In the context of spyware, the regulation seeks to prevent the misuse of such dual-use items for purposes that could violate human rights, including surveillance and repression. Similarly, the Wassenaar Arrangement (WA) „is an international export control regime that aims to promote transparency and greater responsibility in the transfer of conventional arms and dual-use goods and technologies" (Du Bois et al., 2023). In the context of spyware, the WA plays a crucial role in setting out guidelines for the export of surveillance technologies used for both civilian and military purposes. Specifically, the Wassenaar Arrangement includes controls on the export of „intrusion software" and „network surveillance systems" to prevent their misuse for purposes such as unauthorised access to information systems, violation of privacy and human rights abuses. However, several scholars have criticised the aforementioned laws for putting state and commercial interests at the expense of human rights considerations (Riecke, 2023; Phillips, 2023). The EU Parliament's PEGA Committee were also critical of these laws, claiming that they are deliberately too lax when it comes to national implementation (Phillips, 2023). Apart from these laws, there is a palpable lack of regulation at the supranational level on the deployment of spyware. Against this backdrop, despite stiff resistance

from several member states, the EU's attempt to prohibit the use of surveillance technology via EMFA should be applauded[5].

Article 4: A critical examination

The most noteworthy and welcome development of Article 4 EMFA is that the national security derogation has been stripped from the final agreed text, representing a significant coup for advocates of source protection, especially given that spyware has traditionally been justified by citing national security concerns, often serving as a pretext for suppressing dissent (PEGA Committee, 2023). Hitherto, „national security" had been elusively defined in the legislative framework. For instance, the European Convention on Human Rights (ECHR) and the EU Charter do not elaborate on the scope of „national security" (Council of Europe, 2016). Likewise, the definitional scope of „national security" is unclear in both the „Convention 108" (1981) and Directive 2002/58/EC. That said, the explanatory report of the revamped „Convention 108+" provides a more comprehensive albeit vague definition, as per para.91: „the notion of national security should be understood in the sense of protecting the national sovereignty of the concerned Party interpreted having regard to the relevant case-law of the European Court of Human Rights" (Council of Europe, 2016a). Indeed, the EU Agency for Fundamental Rights expressed concern about the lack of clarity regarding the definition of national security, advocating for a broader definition encompassing „major threats to public safety and including cyber-attacks on critical infrastructures" (EU Agency for Fundamental Rights, 2017, p.53). To compound matters, legal interpretations of national security are nationally fragmented which is perhaps unsurprising as it „remains the sole responsibility of each Member State," as per Article 4 of the consolidated version of the Treaty of the European Union. Even so, the principle of subsidiarity – which governs how competences should be allocated between national and supranational levels of governance – is ambivalent as arguably when national security threats have cross-border implications such as organised crime, the EU shares a legal competence with the Member States, as per Article 67(3) of the TFEU (Du Bois et al., 2023; Brogi et al.,2023:51). This raises the important question of which legal framework applies in matters of national security when crime and public safety issues have increasingly cross-border implications. Upon reflection, therefore, the omission of national security from this Article is a remarkable development.

In addition, Art.4 para.4.d provides some form of ex-ante judicial protection, stating that state surveillance measures must be „subject to prior authorisation by a judicial authority or an independent and impartial decision-

[5] Regulating spyware is long overdue particularly given Europe's is such a big player in the spyware industry with four prominent spyware companies based in Europe: *Gamma Group* in the United Kingdom, *FinFisher* in Germany, *Mollitiam Industries* in Spain and *Hacking Team* in Italy (Woodhams, 2021:5).

making authority or in duly justified exceptional and urgent cases, is subsequently authorised by such an authority without undue delay". An ex-ante judicial review provides enhanced checks and balances for MSPs and mitigates the risk of illegitimate state interference. Such a development is not only desirable from a normative perspective but also complies with Art.10 of ECHR[6] aligning closely with the standards established in ECHR jurisprudence – as several scholars pointed out (Voorhoof, 2022). Notwithstanding these welcome developments, it is not clear what would happen in cases where no independent body is available. Presumably, judgment comes back to the national prosecutor which is potentially problematic particularly in countries whose judicial systems have been contaminated politically by ruling parties.

The inclusion of Article 47 of the Charter of Fundamental Rights of the European Union (CFR) safeguards – guaranteeing the right to an effective remedy and a fair trial – is also welcome (Para.8). Thus, under EMFA, the EU ensures that journalists now have the right to an effective remedy before a tribunal. If journalists' rights are violated through the use of spyware (such as their right to privacy, freedom of expression, and protection of journalistic sources), they can take legal action against entities that deploy spyware against them, seeking redress and compensation through the courts. Journalists targeted by spyware have the right to a fair trial by an independent and impartial tribunal. Journalists who may not have sufficient resources to pursue legal action against entities using spyware can access legal aid. This provision ensures that financial constraints do not prevent journalists from seeking justice. Another noteworthy improvement is the revisions made to the „detain-and-intercept" provision (Article 4 para.3a) which is now wider in scope. Importantly, there is now the omission of „on the grounds they refuse to disclose such information". Previously, state intervention was prohibited only in cases where MSPs *refused* to disclose information. However, this implies that interference is allowed when MSPs are not aware of the action or in cases where they do not refuse to provide information (Voorhoof, 2022).

Given the rapidly evolving advancements in surveillance technology, it seems prudent to remove explicit references to „spyware" in Article 4. „Spyware" is replaced by a broader, catchall term, namely „intrusive surveillance software" (Recitals 23, 25-26 and Article 4 para.3c) defined in Article 2 as: „any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enable 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". This definition encompasses a wider range of digital products and activities than spyware; while the latter typically refers to *software* specifically designed to monitor and collect data from a user's device without their knowledge or consent, „intrusive surveillance software" includes any product with digital

[6] The ECHR case of *Sergey Sorokin v. Russia* in 2022 underlined the necessity of ex-ante judicial review to safeguard journalistic sources (Brogi et al.,2023:51).

elements - such as hardware devices, embedded systems, hybrid systems, and digital services - able to exploit vulnerabilities in other digital products for the purpose of covert surveillance. This broader definition acknowledges that not all methods of covert surveillance involve spyware and these technologies are evolving rapidly.

While the step toward harmonising legislation to protect journalistic sources is welcome[7], there are several shortcomings with this article which are laid out below (Brogi et al.,2023:50). The first concern about Article 4 is the provision of retrospective authorisation of intrusive state actions - specifically the „detain-and-intercept" and „forced disclosure" provisions - which countenance the possibility of journalists' rights being violated before the law has been triggered. According to para.4d, Member States may take a state action provided that it is subsequently authorised by a judicial authority or an impartial decision-making authority without undue delay. This begs the question, however, what happens in cases where an action is adjudged as illegitimate, post-facto. In cases such as these, a journalist's rights would have already been violated before the law has stepped in. Authorising state actions retroactively may lead to situations where journalists' rights are violated before proper judicial over-sight, thus undermining the principle of due process. According to National Bureau annual reports, in Bulgaria alone, from 2014-2020, 257 people were placed under surveillance without a prior warrant (ECHR, 2022). This begs the question: how many of these warrants were for legitimate non-politically motivated causes? Although no data is available, it is reasonable to suspect that a significant portion of them were issued illegitimately. This provision also opens the door to potential abuse with states possibly encouraged to conduct intrusive actions in the hope that they can obtain approval afterwards thereby increasing the risk of abuse. In other words, this provision risks tipping the balance of power in favour of the state to the detriment of individual rights such as the right to private life as enshrined in Article 8 of ECHR. It is not clear, furthermore, how promptly an adjudicating body should make a decision for it to satisfy the „undue delay" requirement. The ECHR case, *Ekimdzhiev and Others v. Bulgaria* (2022) is more explicit on what might be considered sufficiently prompt, stating that, „the surveillance operation must stop if the competent judge has not issued a warrant within twenty-four hours" (ECHR, 2022). But even if such a time limit were imposed, it would still allow enough time for the forced - and potentially unlawful - disclosure of information, which could have a detrimental effect on the protection of sources. With this in mind, it might have been preferable to limit judicial authorisation to ex-ante measures, whilst ensuring that judicial decisions are made promptly to assuage any concerns that states may have.

Another concern is that the Article arguably undermines the raison d'ktre of an EU regulation which is to harmonise disparate national regulatory frame-

[7] Especially in light of the increasingly cross-border nature of journalists' work and explicit safeguards against spyware deployment now in place.

works. A case in point is Art. 4 Para 4bii which states that „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*" (emphasis added). This provision is potentially problematic as the list of serious crimes carrying a custodial sentence of 5 years is likely to vary considerably among member states. Furthermore, including Directive (EU) 2016/680 within the scope of Article 4 risks contributing to the fragmentation of EU law, as it delegates the duty to notify national enforcement agencies (EDRi, 2023:3). This reflects a broader pattern of national prerogative trends underpinning this article which risk diluting the effectiveness of the law in addition to eroding the coherence of legal standards across member states. As a corollary to the last point, para. 4a countenances derogations as long as they are provided for in national law; para 4c allows states to deploy intrusive surveillance measures in the case of „overriding public interests". Additionally, paragraphs 4d, 6, and 8, in effect, allows member states to cherry-pick adjudicating bodies whom – while proclaiming to be 'independent' and 'impartial' – might still be more favourable to their cause. Related to this last point is the removal of the stipulation requiring that judicial authorities are 'independent' and/or 'impartial' from the final text. However, a possible implication of this omission is that „public prosecutors with administrative ties to the executive in certain Member States could still qualify for such a crucial control mechanism" (EDRi, 2023:3).

Moreover, although the national security derogation has been removed from the final agreed text, it can reasonably be argued that it has been reintroduced through the backdoor[8]. Paragraph 9 states that „the Member States' responsibilities as laid down in the TEU and the TFEU are respected". This is reaffirmed in Recital 8 which states that: „this Regulation respects the Member States' responsibilities as referred to in Article 4(2) of the Treaty on European Union (TEU), in particular their powers to safeguard essential state functions." Article 4(2) TEU states the following: „The 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." But even if the reference to Article 4(2) is removed, arguably, the law, as it stands, still grants member states wide discretion to invoke national security interests to justify the use of spyware. The inclusion of Para.4.c. states that member states can deploy intrusive surveillance tools so long as it is „by an overriding reason of public interest" – which includes grounds related to *public policy; public security; public safety; and public health*

[8] MEP Clare Daly opined that the national security exemption remains but has merely been reworded (Euractiv, 2023).

(the so-called 'ORPI' principle)[9]. Not only does this give member states even more discretion to deploy spyware, but it can be argued that there is a very fine line between national security and the grounds contained in ORPI (EDRi, 2023). In other words, it is not immediately self-evident what are the main differences between public security and national security grounds, and to my knowledge, EU case law has not specifically addressed this issue[10]. Tellingly, the EU Agency for Fundamental Rights defines national security as „major threats to *public safety* and including cyber-attacks on critical infrastructures," showing the interconnectedness of these terms (EU Agency for Fundamental Rights, 2017:53, emphasis added). If history is any reliable guide, Article 4 is, as it stands, unlikely to detract member states from deploying spyware under the guise of national security (EDRi, 2023; PEGA Committee, 2023).

Another shortcoming of Article 4 is the removal of the prohibition of access to encrypted data, which is becoming an indispensable tool for protecting journalistic sources[11]. The only reference to encrypted data is found in Recital 25 which includes within the broad term of intrusive surveillance software the activity of „access[ing] encrypted content data," as prohibited under Para.3.c. However, as several legal scholars point out, recitals do not hold the same legal weight as article provisions (Klimas et al., 2008). At most, Article 4, para.3 states, albeit rather loosely, that „confidential communications are effectively protected". The explicit outlawing of access to encrypted data was originally proposed in Amendment 109 of the European Parliament's amendments which prohibited „access [of] encrypted content data on any device or in any machine used by media service providers" (Paragraph 2 – point b a). This amendment would have rendered Article 4 more desirable from a journalist's point of view, providing them with a much needed shot in the arm to disseminate and seek confidential information without fear of reprisal thereby ultimately strengthening freedom of expression.

The removal from the final agreed text of the European Parliament's explicit commitment to protecting journalistic sources presents another shortcoming. Initially, as per Article 4 para.2.a, derogations from the „detain-and-intercept" prohibition would have been permissible provided they did not „result in access to journalistic sources" (Amendment 113). The provision reiterates this principle thereupon stating that actors „shall not retrieve data related to the professional activity of media service providers and their employees, in particular

---

[9] Directive 2006/123/EC defines ORPI as „reasons recognised as such in the case law of the Court of Justice, including the following grounds: public policy; public security; public safety; public health; preserving the financial equilibrium of the social security system; the protection of consumers, recipients of services and workers; fairness of trade transactions; combating fraud; the protection of the environment and the urban environment; the health of animals; intellectual property; the conservation of the national historic and artistic heritage; social policy objectives and cultural policy objectives".

[10] EU law has hitherto abstained from explicitly defining these terms.

[11] Indeed, journalists increasingly rely on secure communications to safeguard their sources (Mijatović, 2023).

data which offer access to journalistic sources" (Amendment 113). Thus, previously, an explicit categorical protection was in place barring access to journalistic sources, which is not present in the final agreed text. At most, a positive yet loose commitment states that „Member States shall ensure an effective protection of journalistic sources" (Article 4 para.2a). Similarly, the European Parliament amendment (Article 4.2.a) which states that the 'detain-and-sanction' action may be conducted so long as it „is unrelated to the professional activity of a media service provider and its employees," has been removed, as well. Its omission, in effect, allows member states to carry out politically motivated surveillance. In short, there is ample wriggle room for states to circumvent rules purporting to safeguard journalistic sources (EDRi, 2023: 3).

Another concern with Article 4 is the expansion of the list of serious crimes which would permit member states to derogate from the prohibition of spyware. As per, Para.5.b.i, „Member states may deploy intrusive surveillance software, provided that the deployment is carried out for the for the purpose of investigating one of the persons referred to in paragraph 3, point (c), for: 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". Compared to the original EMFA proposal, the list of crimes has been expanded - by amendments proposed by the Council - providing member states wider discretion to circumvent the surveillance technology ban. Article 2(2) of Framework Decision 2002/584/JHA also includes less serious crimes such as swindling, forgery, intellectual theft, piracy, environmental crime, and also ironically cybercrime. Arguably, these crimes, without downplaying their seriousness, are disproportionate when weighed against the fundamental rights at stake (EDRi, 2023:3). For example, a journalist who downloads streaming content from a pirate website free of charge would be technically breaking intellectual property law. However, based on the reading of Article 4, this would legalise the state deployment of spyware. As a corollary of the last point, it would be interesting to know how many cases - involving journalists who committed crimes in which surveillance technology - had assisted the investigation of a crime. As spyware attacks are covert by their very nature, the precise motivation is rarely known, however, the conclusion of several reports is that the use of spyware mainly politically motivated which makes it all the more necessary that there is a categorical ban on the use of spyware for reasons related to the professional activities of journalists (Council of Europe, 2023b, Carnegie, 2023).

The most concerning ostensible loophole of this Article is that it fails to outlaw the outsourcing of surveillance to private entities. In this regard, the European Parliament's amendments were much more comprehensive. Previously, the range of actors expected to comply with Article 4 was much wider in scope, extending to „Union institutions, bodies, offices and agencies and private entities" (Amendment No. 105 and 106 related to Article 4.2.a). Article 4ccc, furthermore, prohibited commissioning a third party to deploy spyware

which would have helped prevent member states from delegating their „dirty work" to private entities. This was also reaffirmed in the detailed list of derogations pertaining to Article 4.2a which state that: „Member States, including their national regulatory authorities and bodies, Union institutions, bodies, offices and agencies and *private entities* shall not retrieve data related to the professional activity of media service providers and their employees, in particular data which offer access to journalistic sources" (Article 4.2.a, emphasis added). Crucially, the final agreed text does not cover instances in which national governments delegate the deployment of spyware to non-state actors. In cases such as these, the state would not be directly deploying spyware but posing a risk to journalistic sources, nonetheless (Brogi et al.,2023:50). Based on past events, it seems member states are quite willing to outsource certain tasks to private entities. Indeed, according to the CIMA Report, the private surveillance industry is booming, with states increasingly turning to the private sector to acquire off-the-shelf surveillance tools, avoiding the need to invest in developing such technology themselves (Woodhams, 2021:5). For example, during the period of 2011 to 2017, the Mexican government allegedly invested $80 million in technology by the NSO Group, and in 2019, Columbia's military spent $800,000 on spyware from the Spanish company, Mollitiam Industries (Woodhams, 2021:4). According to Privacy International, „more than 500 companies globally now sell 'systems used to identify, track, and monitor individuals and their communications for spying and policing purposes'" (Privacy International, 2018; Woodhams, 2021:4). In the context of disinformation, there is mounting evidence that the Russian government has not only funded disinformation campaigns but outsourced their execution to private troll farms (Euractiv, 2024). This implies that while the state might not be engaging directly in spreading disinformation, they are doing so indirectly by delegating these 'dirty deeds' to public, semi-private or commercial entities (Brogi et al.,2023:50) . This is why it is essential that any future law should include obligations for non-state or private entities as well in order to make the law more watertight against abuse.

Recommendations

In light of the shortcomings highlighted in the previous section, the following recommendations are proposed to enhance the protection of journalistic sources within the EU, aligning with the original aim of Article 4.

- Ideally, a categorical ban on the use of spyware should be introduced unless there are reasonable and compelling grounds to use it such as when investigating a crime with substantial and not spurious evidence (Euronews, 2024). In addition, in the rare circumstance that the use of spyware may be justified, it should only be deployed on matters completely unrelated to the professional activity of the individual under observation.
- To develop a more water-tight and comprehensive anti-spyware regulatory framework, extending to private entities and „quangos" (quasi-autonomous non-governmental organizations") which fall in-between public and private bodies.

- Future regulation should establish a clear affirmative right for journalists to use data encryption to protect confidential sources in line with the 2020 „Council Resolution on Encryption – Security through encryption and security despite encryption" (IPI, 2023). By the same token, future provisions should explicitly outlaw access to journalists' encrypted communications, prohibiting the introduction of „backdoors" into encryption technologies used by journalists. There should also be more support available to journalists and media outlets, particularly the smaller ones with fewer financial resources, incentivising them – via public support programmes or financial incentives – to use encryption technologies.
- As several scholars aptly point out, future EU and national legislation should raise the level of source protection to that which is already guaranteed by ECHR case law (Voorhoof, 2022; EDRi, 2023). ECHR jurisprudence already provides stronger safeguards for individuals subject to surveillance, but it is debatable whether this extends to media service providers in toto.
- The transparency, monitoring, and oversight of spyware technology should be enhanced. More specifically, manufacturers of spyware technology should be obliged to publish a list of their clients and governments should disclose which surveillance tools they are using and why. Regarding the latter, however, in order to not compromise the investigation of a serious crime, rare exceptions on transparency obligations may be granted. Enhanced transparency is also beneficial insofar as it may help victims of unlawful surveillance seek justice (Woodhams, 2021:6-7).
- In addition, manufacturers of spyware should be required to disclose which surveillance tools they are exporting, and to whom, as well as being required to conduct rigorous due diligence checks and vetting assessments to the countries, they are exporting the technology to. Future laws should oblige prospective customers of surveillance technology – whether states or private entities – to disclose the specific purposes and intended use cases for the technology. This information should be publicly available and exposed to rigorous oversight checks at the EU level so that state actions can be easily monitored.

Bibliography:

- Access Now. (2023, September 13). *Hacking Meduza: Pegasus spyware used to target Putin's critic.* https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/
- Akin Gump Strauss Hauer & Feld LLP. (2021). The Recast dual use regulation - a missed opportunity. Akin Gump Strauss Hauer & Feld LLP - the Recast Dual Use Regulation - a Missed Opportunity. https://www.akingump.com/en/insights/alerts/the-recast-dual-use-regulation-a-missed-opportunity

- Bátorfy, A, Bleyer-Simon, K, Szabó, K, Galambosi, E (2022). Monitoring media pluralism in the digital era : application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2021. Country report : Hungary. Centre for Media Pluralism and Media Freedom (CMPF), Media Pluralism Monitor (MPM), Country Reports - https://hdl.handle.net/1814/74692
- Bleyer-Simon, K., Brogi, E., Carlini, R., Da Costa Leite Borges, D., Kermer, J.E., Nenadic, I., Palmer, M., Parcu, P. L., Trevisan, M., Verza, S., & Žuffová, M. (2024). Monitoring media pluralism in the digital era: Application of the media pluralism monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2023. European University Institute, Robert Schuman Centre for Advanced Studies, Centre for Media Pluralism and Media Freedom (CMPF).
- Bradshaw, P. (2020). Chilling Effect: Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations. In Journalism, Citizenship and Surveillance Society (pp. 79-97). Routledge.
- Brogi, E., Borges, D., Carlini, R., Nenadic, I., Bleyer-Simon, K., Kermer, J. E, Reviglio Della Venaria, U., Trevisan, M., & Verza, S. (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. https://hdl.handle.net/1814/75938 Retrieved from Cadmus, EUI Research Repository.
- Carnegie Endowment for International Peace. (2023). *Why does the global spyware industry continue to thrive? Trends, explanations, and responses*. https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en
- Centre of Media Pluralism and Media Freedom. (2024). EMFA in focus: towards a common regulatory framework to foster media pluralism? European University Institute. https://www.eui.eu/events?id=566849
- CMPF. (2024). *EMFA in focus: towards a common regulatory framework to foster media pluralism?* European University Institute. https://www.eui.eu/events?id=566849
- Committee to Protect Journalists. (2023, September 22). Two Prague-based Russian journalists threatened, fear surveillance. https://cpj.org/2023/09/two-prague-based-russian-journalists-threatened-fear-surveillance/
- Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Council of Europe. https://rm.coe.int/1680078b37
- Council of Europe - Safety of Journalists Platform. (2023). *Safety of journalists*. https://fom.coe.int/en/alerte/detail/107639877;globalSearch=false
- Council of Europe. (2016a). Draft explanatory report - Convention 108 modernised [Report]. Retrieved from https://rm.coe.int/convention-for-the-protection-of-individuals-with-regard-toautomatic-/16806b6ec2
- Council of Europe. (2023b, September 20). Pegasus and similar spyware and secret state surveillance (Doc. 15825 Report). Committee on Legal Affairs and Human Rights. Rapporteur:

Mr. Pieter Omtzigt, Netherlands, Group of the European People's Party. Retrieved from https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68

- Council of Europe. (2024c, February 13). Encryption in the age of surveillance. Commissioner for Human Rights. https://www.coe.int/en/web/commissioner/-/encryption-in-the-age-of-surveillance
- Du Bois, R., Reyes, A. T. (2023). Dual-use and cyber-surveillance: EU policies and current practices [INTA committee report]. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754439/EXPO_BRI(2023)754439_EN.pdf
- Euractiv. (2024, March 14). EU Parliament passes European Media Freedom Act, concerns over spyware remain. *www.euractiv.com*. https://www.euractiv.com/section/media/news/eu-parliament-passes-european-media-freedom-act-concerns-over-spyware-remain/
- Euronews. (2024, March 13). Will the Brussels spyware scandal finally convince the EU to act? *Euronews*. https://www.euronews.com/my-europe/2024/03/13/will-the-brussels-spyware-scandal-finally-convince-the-eu-to-act
- European Court of Human Rights. (2022). Ekimdzhiev and Others v. Bulgaria (Application No. 70078/12). https://hudoc.echr.coe.int/fre?i=001-214673
- European Digital Rights (EDRi). (2023, October 3). *Encryption in the age of surveillance - European Digital Rights (EDRi)*. https://edri.org/our-work/event-summary-encryption-in-the-age-of-surveillance/
- European Union Agency for Fundamental Rights. (2017) 'Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU. Volume II: Field perspectives and legal update', Publications Office of the European Union, at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-servicesvol-2_en.pdf
- Feldstein, S., & Kot, B. (2023, March 1). Explaining the resilience of the global spyware and digital forensics industry. Carnegie Endowment for International Peace, 137(3476), 980-980. https://doi.org/10.1038/137980d0
- Fowler, A. (2018). Shooting the Messenger: Criminalising Journalism (1st ed.). Routledge. https://doi.org/10.4324/9781315099927
- Freedom House. (2023). Crime and punishment: the twin threats faced by journalists in Central America. Freedom House. https://freedomhouse.org/article/crime-and-punishment-twin-threats-faced-journalists-central-america
- https://vtechworks.lib.vt.edu/server/api/core/bitstreams/7ddfc7ac-400f-4690-8e52-cffec44dbc5b/content
- IPI. (2023). IPI position on the European Media Freedom Act. ipi.media. Retrieved May 28, 2024, from https://ipi.media/ipi-position-on-the-european-media-freedom-act/
- Klimas, T., & Vaiciukaite, J. (2008, July 14). The law of recitals in European Community legislation. ILSA Journal of International & Comparative Law, 15. Retrieved from SSRN: https://ssrn.com/abstract=1159604
- Luyten, K., and Rossi, A., 'Understanding the EU's response to organised crime (Briefing No. PE 652.043)', Parliamentary Research Service, 2022, at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652043/EPRS_BRI(2020)652043_EN.pdf

- PEGA Committee. (2023). The impact of Pegasus on fundamental rights and democratic processes (Study). European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf
- Phillips, R. (2023). The Efficacy of European Union Spyware Regulations. Virginia Tech. Tech Humanity Lab. https://vtechworks.lib.vt.edu/server/api/core/bitstreams/7ddfc7ac-400f-4690-8e52-cffec44dbc5b/content
- Privacy International. (2018). The global surveillance industry. Retrieved May 28, 2024, from https://privacyinternational.org/explainer/1632/global-surveillance-industry
- Riecke, L. (2023). Unmasking the term 'dual use' in EU spyware export control. European Journal of International Law, 34(3), 697-720. https://doi.org/10.1093/ejil/chad039
- Rožukalne, A., & Skulte, I. (2024). Monitoring media pluralism in the digital era: Application of the media pluralism monitor in the European member states and in candidate countries in 2023. Country report: Latvia. Centre for Media Pluralism and Media Freedom (CMPF), EUI, RSC. https://hdl.handle.net/1814/77007
- Sophie in 't Veld, (2023, May 22). European Parliament draft recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware. https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html
- Štětka, V., Adamčíková, J., & Sybera, A. (2024). *Monitoring media pluralism in the digital era: Application of the media pluralism monitor in the European member states and in candidate countries in 2023. Country report: The Czech Republic*. Centre for Media Pluralism and Media Freedom (CMPF), EUI, RSC. https://hdl.handle.net/1814/77020
- Voorhoof, D. (2022). European Media Freedom Act and the protection of journalistic sources: still some way to go, The International Forum for Responsible Media Blog (Inforrm), available at: https://inforrm.org/2022/11/18/european-media-freedom-act-and-the-protection-of-journalisticsources-still-some-way-to-go-dirk-voorhoof/
- Wasserman, E. (2017). Safeguarding the News in the Era of Disruptive Sources. Journal of Media Ethics, 32(2), 72-85. https://doi.org/10.1080/23736992.2017.1294020
- Woodhams, S. (2021). Spyware: An unregulated and escalating threat to independent media. Center for International Media Assistance. https://www.cima.ned.org/wp-content/uploads/2021/08/CIMA_Spyware-Report_web_150ppi.pdf