Module 4

Surveillance of Journalists, Searches and Digital Device Seizures

Modules on Digital Rights and Freedom of Expression Online in Europe

MEDIA DEFENCE

ISBN 978-0-9935214-1-6
Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Published in May 2024

TABLE OF CONTENTS

MODULE 4

1. INTRODUCTION

Safeguarding the rights of journalists in the digital space, including protecting their communications and other sensitive data, has become an increasingly complex and relevant issue in the new information age. As the usage of the Internet, including online communication tools and electronic data sharing platforms, expand rapidly, a growing amount of data is transferred and stored digitally. In addition, many contributions to public debate are disseminated and received online.

While legislative, judicial and policy developments are struggling to keep up with the fast pace of technological developments, European countries and regional organisations, such as the European Union (EU) and the Council of Europe (CoE) have introduced measures addressing both old standing as well as emerging questions relating to privacy, security and freedom of expression. These include questions around the surveillance and retention of journalists' communications and other forms of access to their devices.

2. SURVEILLANCE: BULK DATA INTERCEPTION

Surveillance of communications, including by introducing bulk interception regimes, has been to the forefront of legal developments on the issue of surveillance in recent years. Not only the increased data flow online, but also the technical sophistication of surveillance tools increases the risk of citizens, including journalists, becoming "transparent persons"[1] for state authorities. According to the UN Special Rapporteur on freedom of expression:

> "Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. […] As such, the State now has greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."[2]

2.1. What is bulk data interception?

Bulk data interception is defined as "the gathering of large chunks of internet traffic from around the world" in situations where the target is unknown, and the intent of the measure is to discover rather than to investigate.[3] The data gathered can include, besides the content of the communication, the circumstances of its transmission, including the "who", "when" and "where".[4] It is closely linked to mass surveillance, which "involves the acquisition, processing, generation, analysis, use, retention or storage of information about large numbers of people, without any regard to whether they are suspected of wrongdoing."[5]

---

[1] This term, which was originally used the debates around the 1982 German census law, describes the extensive collection of personal data by public authorities.
[2] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (17 April 2013), para 33, A/HRC/23/40, (accessible here).
[3] Big Brother Watch, Interception (undated) (accessible here).
[4] Nóra Ní Loideáin, Bulk Surveillance: Europe's Recent Landmark Judgements (5 July 2021), (accessible here).
[5] Privacy International, Mass Surveillance (undated), (accessible here),

Such practices – as well as targeted surveillance measures – infringe on the right to privacy (Article 17 ICCPR, Article 8 ECHR), as authorities gain access to intimate private and professional data. In addition, the knowledge – or even suspicion – of being surveilled undermines the right to freedom of expression (Article 19 ICCPR, Article 10 ECHR), as the fear of unwillingly disclosing online activity or the identity of journalistic sources creates a chilling effect and leads to self-censorship, in particular in repressive environments.

2.2. International legal standards

Various UN bodies have expressed concern over the human rights impact of surveillance measures. For instance, the UN Human Rights Committee has stated that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[6] It further stated that to comply with the requirements of Article 17 ICCPR, the right to privacy, the "integrity and confidentiality of correspondence should be guaranteed de jure and de facto."[7]

Communications surveillance has been described as a "highly intrusive act" which can only be justified in the most exceptional circumstances and must be accompanied by sufficient safeguards.[8] Beyond this – as criticised by the UN Special Rapporteur on counter-terrorism in 2014 – "[b]ulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17 [ICCPR]"[9] as it "eradicates the possibility of any individualized proportionality analysis."[10] Aligned with this assessment, the UN Office of the High Commissioner for Human Rights (OHCHR) has also stressed that indiscriminate mass surveillance, and communications interception, collecting, storing and analysing of all users, is "not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures."[11] According to the OHCHR, "the mere possibility of communications information being captured" and thus the very existence of a mass surveillance programme, interferes with the right to privacy.[12]

---

[6] UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) (1988), para 8, HRI/GEN/1/Rev.1 (accessible here).
[7] *Ibid.*
[8] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (17 April 2013), para 81, A/HRC/23/40, (accessible here) available at
[9] Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Promoting and protecting human rights and fundamental freedoms while countering terrorism (23 September 2023), A/69/397, paras 47 and 59.
[10] Ibid. para 12.
[11] UN OHCHR, Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism (21 July 2016), A/HRC/33/29, para 58, (accessible here) available at; see also: UN OHCHR, The right to privacy in the digital age (3 August 2018), A/HRC/39/29, para 17, (accessible here).
[12] UN OHCHR, The right to privacy in the digital age (30 June 2014), A/HRC/27/37, para 20,(accessible here)

2.3. Regional standards: EU

For almost a decade, mass surveillance measures have been subject to interpretation by European courts. The Court of Justice of the European Union (CJEU), in particular, has dealt with the topic of data retention measures extensively in a number of landmark judgments, raising concerns about, inter alia, the fact that the retained data allows authorities to draw very precise conclusions about the private life of the individuals concerned.[13]

- In its judgment regarding the case Digital Rights Ireland/Seitlinger and Others (2014), the CJEU invalidated the Data Retention Directive (EU Directive 2006/24/EC), which, inter alia, required telecommunications providers to retain all users' traffic and location data for prolonged periods. The CJEU invalidated the Directive on the basis that it interfered with the right to respect for private and family life and the protection of personal data in a "particularly serious" and disproportionate manner.[14]

- Two years later, in Tele2 Sverige AB/Watson and Others (2016), the CJEU built on these findings, holding that EU law precluded domestic legislation imposing an obligation on electronic communications services to generally and indiscriminately retain traffic and location data for the purpose of fighting crime.[15] The CJEU at the same time clarified that the targeted retention of data, limited to what is strictly necessary, and imposed by clear and precise legislation containing sufficient safeguards is not precluded by EU law.[16]

- In the case of Privacy International (2020), the CJEU reiterated the prohibition of general and indiscriminate retention of data. The case required it to consider the application of EU law to domestic legislation requiring communications service providers to retain data and/or forward it to national security and intelligence services.[17] The CJEU expanded on its findings in the Tele2 case, holding that EU law precludes domestic legislation which requires electronic communication service providers to generally and indiscriminately transmit traffic and location data to *security and intelligence agencies* for the purpose of safeguarding national security.[18] In the joined case of La Quadrature du Net and Others (2020), the CJEU held that an order requiring general and indiscriminate location and traffic data retention can be justified where the state is facing

[13] See for instance CJEU, Judgment of the Court (Grand Chamber) concerning SpaceNet AG and Telekom Deutschland GmbH v Bundesrepublik Deutschland (20 September 2022), paras 117 and 184.
[14] CJEU, Judgment of the Court (Grand Chamber) concerning Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources and Others and Kärtener Landesregierung and Others, Joined Cases C-293/12 and C-594/12 (8 April 2014), paras 37 and 69.
[15] CJEU, Judgment of the Court (Grand Chamber) concerning Tele2 Sverige AB v Post- ich telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Joined Cases C-203/15 and C-698/15 (21 December 2016), para 112.
[16] Ibid. para 108.
[17] CJEU, Judgment of the Court (Grand Chamber) concerning Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, Case C-623/17 (6 October 2020), para 82.
[18] Ibid. para 49; see for an analysis for instance Monika Zalnieriute, A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence (4 June 2021), (accessible here) and Juraj Sajfert, Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy (26 October 2020), (accessible here).

a serious, genuine and present or foreseeable threat to national security.[19] While this order must be limited in time to what is strictly necessary, it may be extended if the threat persists.[20] Additionally, the CJEU clarified requirements for targeted retention as well as retention of IP addressed and other data allowing the identification of users, classifying some types of data as "less sensitive"[21].

- It its recent decision in the case SpaceNet/Telecom Deutschland (2022), the CJEU again confirmed that EU law precludes the requirement of preventive, general and indiscriminate data retention to combat serious crime and prevent serious threats to public security.[22] It further elaborated on a number of measures which, insofar as they are established by clear and precise rules containing sufficient safeguards, are not precluded, including:[23]

    - Instructions to generally and indiscriminately retain traffic and location data for the purpose of safeguarding national security where there is a serious, genuine, present and foreseeable threat to national security, insofar as an effective review process is in place and the instruction is limited in time to what is strictly necessary;
    - Targeted retention of traffic and location data, which is limited in time and scope, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security;
    - In addition, the CJEU elaborates on the circumstances under which the indiscriminate and general retention of IP addresses, data relating to the civil identity of users and expedited retention of traffic and location data in the possession of service providers may be justified under EU law.

2.4. Regional standards: CoE

The European Court of Human Rights (ECtHR) has also assessed the legality of different domestic bulk interception systems in several landmark cases.

Initially, in the 2006 judgment in the case *Weber and Saravia v. Germany*, the ECtHR held that states generally enjoy a "fairly wide margin of appreciation" in respect to measures concerning national security and the prevention of crimes.[24]

A few years later, the ECtHR had to examine the Russian secret telecommunications regime in light of the ECHR in *Zakharov v. Russia*. The Grand Chamber found a violation of Article 8 ECHR, arguing that the domestic provisions lacked "adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance".[25] Similarly, the ECtHR found that the Hungarian anti-terror legislation did not

[19] CJEU, Judgment of the Court (Grand Chamber) concerning La Quadrature du Net and Others v Premier minister and Others, Joined Cases C-511/18, C-512/18 and C-520/18 (6 October 2020), para 168.
[20] *Ibid.*
[21] *Ibid*. paras 152, 168.
[22] CJEU, Judgment of the Court (Grand Chamber) concerning SpaceNet AG and Telekom Deutschland GmbH v Bundesrepublik Deutschland (20 September 2022), para 132.
[23] *Ibid.*
[24] ECtHR, *Weber and Saravia v. Germany*, App. No. 54934/00, §137, 29 June 2006.
[25] ECtHR, *Roman Zakharov v Russia* [GC], App No. 47143/06, §302, ECHR 2015.

contain sufficient safeguards and expressed its concern over the fact that virtually anyone in Hungary could be surveilled.[26]

In a groundbreaking judgment on bulk surveillance, the ECtHR's First Section ruled in *Big Brother Watch v. UK* in 2018 that bulk interception by intelligence agencies is not in and of itself incompatible with the right to privacy.[27] This finding was later confirmed by the Grand Chamber, which found that bulk interception measures can be justified under certain circumstances, such as for gathering intelligence data and to counter terrorism and espionage.[28] The ECtHR held that while bulk interception regimes do not *per se* violate the Convention rights, they must contain end-to-end safeguards as well as sufficient protection for journalistic sources.[29] In the case of *Centrum för Rättvosa v. Sweden*, decided on the same day, the ECtHR's Grand Chamber found that the Swedish bulk interception regime violated Article 8 ECHR, but also explicitly held that "bulk interception is of vital importance to Contracting States in identifying threats to their national security" and "no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power."[30]

The Court has since examined further domestic mass surveillance and data retention systems and found violations of the ECHR.[31]

2.5. Litigating bulk data interception cases: Victim status

The term "standing" is usually understood as a person's or organisations ability to bring a case to a particular court. While its requirements differ between jurisdictions, an applicant is usually asked to establish why they are affected by the matter or what interest they represent. Often, they will be required to demonstrate a sufficient connection between an issue and their interest in it.

The ECtHR, as mandated by Article 34 ECHR, accepts applications from those "claiming to be a victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto." While this includes not only direct victims also those who would suffer harm or have a valid interest in the case,[32] the ECtHR has made clear that:

> "the Convention does not provide for the institution of an *action poularis* and that its task is not normally to review the relevant law and practice *in abstracto*, but to determine

[26] ECtHR, *Szabó and Vissz v. Hungary*, App. No. 37138/14, §88, 12 January 2016.
[27] ECtHR, *Big Brother Watch and Others v. the United Kingdom*, App Nos. 58170/13 and 2 others, §314, 13 September 2018; see for an analysis Nóra Ní Loideáin, Bulk Surveillance: Europe's Recent Landmark Judgements (5 July 2021), (accessible here).
[28] ECtHR, *Big Brother Watch v. UK*, App Nos. 58170/13 and Others, 25 May 2021; see for an analysis Eliza Watt, The legacy of the privacy versus security narrative in the ECtHR's jurisprudence (21 April 2022) (accessible here).
[29] ECtHR, *Big Brother Watch v. UK*, App Nos. 58170/1 and Others, §§350, 442-450, 25 May 2021.
[30] ECtHR, *Centrum för Rättvisa v. Sweden*, App. No. 35252/08, §365, 25 May 2021; Monika Zalnieriute, A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence (4 June 2021), (accessible here).
[31] See for instance ECtHR, *Ekimdziev and Others v. Bulgaria*, App. No. 70078/12, 11 January 2022; ECtHR, *Podchasov v. Russia*, App. No. 33696/19, 13 February 2024; ECtHR, Škoberne v. Slovenia, App No. 19920/20, 15 February 2024.
[32] ECtHR [GC], *Vallianatos and Others v. Greece, App*. Nos. 29381/09 and 32684/08, §47, 7 November 2013.

> whether the manner in which they were applied or affected the applicant gave a rise to a violation of the Convention."[33]

Therefore, the ECtHR generally requires applicants to explain how they were victims of a specific act that they claim violated their rights. However, under certain circumstances, "potential victims" can apply to the ECtHR. This includes individuals suspecting to have been targeted by covert (surveillance) measures. As these individuals cannot know whether such a measure was used, the ECtHR accepts that "the mere existence of secret measures or of legislation permitting secret measures" can may sufficient.[34] This the case where the applicant can possibly have been affected by the legislation in question and there are no sufficient and effective domestic remedies available.[35]

Similar approaches are taken by some domestic court. For example, the Federal Constitutional Court of Germany accepted the submission that the applicants, who had complained of the 2007 retention obligations in the Telecommunications Act, used telecommunication services in their private and professional capacity, accepting their standing based on the "reasonable likelihood" of being affected of such measures.[36] The Constitutional Court continued to follow this line of argument in subsequent cases, where there was a sufficient probability of the applicants having been targeted with measures under the provisions complained of when there were insufficient ex post facto disclosure obligations.[37]

3. SURVEILLANCE: SPYWARE

Targeted surveillance describes surveillance which focusses on obtaining information about the communications of a specific individual, such as a person who is already a suspect in a criminal case."[38] A prominent example is the use of spyware, a malicious type of software which "interferes with a device's normal operation to collect information without alerting the user".[39]

The most intrusive type of spyware currently known to the public is Pegasus spyware, which is manufactured by the Israeli cyber-arms company NSO Group and is exclusively sold to governments. In 2021, the Organised Crime and Corruption Project (OCCPR), released a report which outlined the use of Pegasus spyware on, inter alia, journalists, human rights defenders, activists and political figures worldwide.

---

[33] ECtHR, *Roman Zakharov v Russia* [GC], App No. 47143/06, §164, ECHR 2015 with further references.
[34] See ECtHR, Klass and Others v. Germany, App No. 5029/71, §34, 6 September 1978.
[35] ECtHR, *Roman Zakharov v Russia* [GC], App No. 47143/06, §171, ECHR 2015; see also ECtHR, Kennedy v. UK, App No. 26839/05, §124, 18 May 2010; ECtHR, Centrum för Rättvisa v. Sweden, App. No. 35252/08, §§166-167, 25 May 2021; ECtHR, *Wieder and Guarnieri v. The United Kingdom*, App Nos. 64371/16 and 64407/16, §§97-110, 12 September 2023.
[36] German Federal Constitutional Court, Order of 2 March 2010 (TKG), 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08, §§177-178, (accessible here).
[37] German Federal Constitutional Court, Order of 20 April 2016, 1 BvR 966/09, §§82-84, (accessible here) and Order of 19 May 2020, BNDG, 1 BvR 2835/17, §§71-76, (accessible here).
[38] Nóra Ní Loideáin, Bulk Surveillance: Europe's Recent Landmark Judgements (5 July 2021), (accessible here).
[39] Amnesty International, What is spyware and what can you do to stay protected? (14 December 2023), (accessible here).

Pegasus spyware can be installed covertly on an individual's device, often their mobile phone. Once installed, the spyware turns the device into a full-time surveillance tool, granting unrestricted access to the stored data, as well as the device's camera, microphone, messages, photos, passwords, calls, and geolocation

Methods of implantation on a device include the clicking on a malicious link by the user or the use of a wireless transmitter in close proximity to the phone. However, one of the most concerning revelations about Pegasus spyware is its capability to infect a device through the so-called "zero click"-method, which does not require any act by the user or any "jailbreaking" of the system.

Once a device is infected, it is extremely difficult to detect the spyware as well as its actions, for instance whether there has been an extraction of data.

3.1. International standards

Various international bodies have expressed serious concern over the use of spyware, including the UN Human Rights Committee.[40] As pointed out by the UN OHCHR, the development and use of pervasive surveillance tools is "profoundly alarming", threatening the rule of law and eroding pluralistic democracies.[41] The targeting of journalists, human rights defenders and others with this spyware tool constitutes a serious interference with the right to privacy (Article 17 ICCPR)[42] which, in particular when carried out for political reasons, can never be justified[43].

In addition, the use of Pegasus spyware violates freedom of expression, protected on the international level by Article 19 ICCPR. Infecting a personal communication device with spyware permits "insights into the thinking processes of individuals subject to hacking, as well as their political and religious views and beliefs".[44] This is especially true in the journalistic context as the protection of journalistic sources is circumvented and the mere existence of spyware creates a chilling effect.[45]

3.2. Regional standards: EU

In the EU, targeted surveillance measures – with the exception of national security measures excluded from its scope by Article 4(2) TEU – must comply with applicable Union primary and secondary law, in particular the EU Charter, the ePrivacy Directive and the Law Enforcement

[40] HRC, *Concluding observations on the seventh periodic report of Germany* (30 November 2021), CCPR/C/DEU/CO/7, paras 42-43, (accessible here); HRC, *Concluding observations on the fifth periodic report of the Netherlands* (22 August 2019), CCPR/C/NLD/CO/5, paras 54-55, (accessible here); HRC, *Concluding observations on the sixth periodic report of Italy* (1 May 2017), CCPR/C/ITA/CO/6, paras 36-37, (accessible here).
[41] UN Human Rights Council, *The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights* (4 August 2022), A/HRC/51/17, para 54, (accessible here).
[42] *Ibid*. paras 4-5 and 9, (accessible here).
[43] *Ibid*. paras 18-19.
[44] Ibid, para 9, (accessible here); see also Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (22 May 2015), A/HRC/29/32, para 20, (accessible here).
[45] *Ibid*. para 10.

Directive.[46] Article 52(1) EU Charter requires all acts limiting fundamental rights to confirm with the requirements of proportionality and necessity. [47]

Due to the quality and quantity of data stored on smartphones, the EU Data Protection Supervisor, considers it "highly unlikely that spyware such as Pegasus, which de facto grants full unlimited access to personal data, including sensitive data, could meet the requirements of proportionality" as "the interference with the right to privacy is so severe that the individual is in fact deprived of it" and that the protection of third parties and those who are afforded special protection, such as lawyers, is not guaranteed.[48]

In a similar approach, the European Parliament has condemned "the use of spyware by Member State governments, and members of government authorities or state institutions for the purpose of monitoring, blackmailing, intimidating, manipulating and discrediting opposition members, critics and civil society, eliminating democratic scrutiny and the free press, manipulating elections and undermining the rule of law by targeting judges, prosecutors and lawyers for political purposes."[49]

3.3. Regional standards: CoE

On 23 October 2023, the CoE's Parliamentary Assembly issued a resolution expressing its deep worry about "mounting evidence that Pegasus and similar spyware have been used illegally or for illegitimate purposes by several member states, including against journalists, political opponents, human rights defenders and lawyers" and condemned its use for political purposes.[50]

Even before the revelations about the intrusiveness of Pegasus spyware, ECtHR's Grand Chamber has acknowledged that against the backdrop or rapid technical advancement, domestic law must be sufficiently clear "to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."[51]

The ECtHR has yet to deliver its first judgment on a case concerning the use of Pegasus spyware. However, its caselaw gives some insights into how it approaches such matters.

The use of intrusive spyware against journalists goes to the heart of their right to private and family life (Article 8 ECHR), as well as their freedom of expression (Article 10 ECHR), as it gives access to a range of sensitive information and correspondence and creates a chilling effect for those contributing to public debate. Its use fails to meet the conditions of the so-called three-part test, in particular the requirements of necessity and proportionality. Lastly, Pegasus spyware circumvents the protection of journalistic sources, without which, as

[46] See: The European Data Protection Supervisor, Preliminary Remarks on Modern Spyware (15 February 2022), p. 6, (accessible here).
[47] Ibid. p. 7.
[48] The European Data Protection Supervisor, Preliminary Remarks on Modern Spyware (15 February 2022), p. 8, (accessible here).
[49] EU Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation) (15 June 2023), no. 3, (accessible here).
[50] PACE, *Pegasus and similar spyware and secret state surveillance, Resolution 2513 (2023)* (11 October 2023), (accessible here).
[51] *Roman Zakharov v Russia* [GC], App No. 47143/06, §229, ECHR 2015.

stressed by the ECtHR, sources may be deterred from speaking to the press, which in turn cannot fulfil its public watchdog role.[52]

Litigating spyware cases: Victim status

In contrast to cases concerning mass surveillance legislation, individuals targeted with spyware, such as Pegasus spyware, have usually been informed by technical experts, their devices' manufacturer or civil society organisations that they have been specifically targeted and that their devices have been infected. However, they often face other obstacles in litigating their cases, as the majority of the information about the hacking remains solely in the domain of the attacking state. These difficulties include, but are not limited to the following:

- Meeting the burden of proof required by the court they are accessing;
- Difficulties in obtaining detailed technical evidence that the hacking took place;
- Submitting details on the date and length of the infection, the data accessed/extracted and the aim of the measure;
- Identifying the attacking state.

4. SEARCHES AND DEVICE SEIZURE

Digital devices such as phones, cameras, laptops, and storage devices have become essential tools for journalists in conducting their work. They are used, for instance to conduct for research, recording, communicating with confidential sources and other journalists, and for publishing content. However, such devices often become subject to seizures and searches by authorities, in particular in situations perceived as sensitive, such as when covering protests[53] or at national borders[54]. As civil society organisations are documenting growing number of seizures and (forensic) searches of journalists' digital equipment,[55] safeguarding digital security remains an important factor to ensure the functioning of the press. Practical tips for journalists covering protests can be found here.

Through searches and seizures, authorities obtain access to protected materials, including the identity of journalistic sources, thus endangering their safety and creating a chilling effect. The search of mobile devices is particularly intrusive due to the quantity and the sensitivity of the data accessed. Such measures infringe on the right to privacy (Article 8 ECHR) and freedom of expression (Article 10 ECHR) and can only be justified if they meet the cumulative criteria of the so-called three-part test. In addition, the search of journalists' home, workplace and the seizure of their material must be accompanied by adequate and effective procedural safeguards.[56]

[52] See for instance ECtHR, Telegraaf Media Nederland Landelijke Media B.V. and Others v. The Netherlands, App No 39315/06, §127 22 November 2012; ECtHR, Sedletska v. Ukraine, App No. 42634/18, §§54-55, 1 April 2021.
[53] See for instance Media Defence, Reporting at Protests: Factsheet (undated), (accessible here).
[54] See for instance Article 19, European Court of Human Rights: Search of journalists' devices at border (31 August 2023), (accessible here).
[55] For example in West Africa: MFWA, Seizure and Destruction of Journalsits' Digital Tools: The Data Privacy and Censorship implications (2 April 2020), (accessible here).
[56] CoE Platform to promote the protection of journalism and safety of journalists, The Protection of Journalistic Sources, A Cornerstone of the Freedom of the Press (June 2018), (accessible here).

The ECtHR has clarified that:

> "journalists should enjoy a broad scope of protection, including a range of freedoms that are of functional relevance to the pursuit of their activities, such as: protection of confidential sources; protection against searches of professional workplaces and private domiciles and the seizure of materials, protection of news and information-gathering processes […]"[57]

Special attention must be paid to the protection of journalistic sources,[58] a principle which, in the words of the ECtHR, is "one of the cornerstones" of press freedom and essential to enable the press to fulfil its public-watchdog role.[59]

The ECtHR has applied these numerous cases, confirming for instance that the search of a journalist's laptop at a border crossing violated Article 8 ECHR due to the lack of effective and adequate safeguards in Russian domestic legislation and practice.[60] In *Sorokin v. Russia*, the ECtHR found a violation of Article 10 ECHR after a journalist's flat and his electronic devices, which contained information related to his work, were searched without any procedural safeguards to protect the confidentiality of his sources.[61] In *Nagla v. Latvi*a, the ECtHR stressed that:

> "the right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources, but is part and parcel of the right to information, to be treated with the utmost caution"[62].

[57] ECtHR, *Man and Others v. Romania*, App. No. 39273/07, §131, 19 November 2019.
[58] See for instance CoE Committee of Ministers, Recommendation No. R (2000) 7 of the Committee to Ministers to member states on the right of journalists not to disclose their sources of information (8 March 2000), (accessible here).
[59] ECtHR, *Sedletska v. Ukrain*e, App No. 42634/18, §§54-55, 1 April 2021; see also ECtHR, Telegraaf Media Nederland *Landelijke Media B.V. and Others v. The Netherlands*, App No 39315/06, §127 22 November 2012; ECtHR, *Goodwin v. The UK*, App No. 17488/90, §39, 27 March 1996.
[60] ECtHR, *Ivashchenko v. Russia*, App. No. 61064/10, §§63-69, 93, 13 February 2018.
[61] Dirk Vorhoof, European Court of Human Rights: Sergey Sorokon v Russia (2022), (accessible here).
[62] ECtHR, *Nagla v. Latvia*, App No 73469/10, §97, 16 July 2013.