REPORTERS WITHOUT BORDERS

Recommendations on the Greek legal framework on surveillance

November 2022

Summary of recommendations

1. Lack of judicial oversight in cases of surveillance on national security grounds

- ➔ Allow for an independent judicial overview of requests for surveillance by security services, and for an independent judicial authority to authorize such requests, including in cases where a breach of national security is alleged.
- ➔ Oblige security forces to justify the request for surveillance, in order for judicial review to assess whether it complies with the principles of legality, necessity and proportionality.
- ➔ Ensure not only the independence, but also the effectivity, of the oversight of the necessity and proportionality of the requested surveillance
- ➔ Repeal the recent amendment to the law that prevents individuals from being informed of the fact they were submitted to surveillance, to ensure they can exercise their right to effective remedy.

2. Lack of safeguards against abuse of surveillance

- ➔ Provide for a proportionate limitation of the period during which an individual can be placed under surveillance on grounds of national security, in line with the case law of the ECtHR.
- ➔ Limit by law the types of communications that may be intercepted and the means by which the interception may be performed.
- ➔ Ensure that information collected are only those relevant to an alleged perpetration or preparation of a crime.
- ➔ Provide for a procedure of destruction of data collected when investigations on alleged breaches of national security did not confirm such allegations, under the control of an independent authority or a judicial authority

3. Lack of specific safeguards against surveillance of journalists

- ➔ Provide for specific guarantees in cases where surveillance is requested against a journalist : protection of journalistic sources, strengthening of the judicial oversight, protection against incidental surveillance

4. lack of sufficient legal framework on the use of spyware

- ➔ Transparency of the use of spywares
- ➔ compliance of the use of spyware with the above stated guarantees

5. Vague definition of national security

- ➔ Review the legislation on national security, to ensure that the conditions allowing for surveillance on its ground meet the requirements of legitimacy, necessity and foreseeability.
- ➔ At the minimum, the legislation should define what constitutes a breach to national security, and provide for a definition of the categories of people that may be considered a threat to national security, and the objects which may be placed under surveillance.

The recent cases of surveillance of two journalists in Greece, Thanasis Koukakis and Stavros Malichudis, have revealed worrying insufficiencies of the Greek legal framework on surveillance and lack of guarantees for the respect of Human Rights and journalistic freedoms, as regard international standards and the case law of the European Court of Human Rights : in particular the lack of sufficient judicial overview and the absence of specific guarantees against the surveillance of journalists on the basis of the right to confidentiality of sources. These concerns have been further exacerbated by the October 2022 revelation of the alleged tracking through their phones of the movement of Thanasis Koukakis and three other journalists investigating the surveillance scandal.

The European Court of Human Rights (ECtHR), in a recent judgment that addresses the issue of breaches of confidentiality of communications of individuals on national security grounds, has considered that **six "minimum safeguards"** should be set out in law to avoid abuses of power in the interception of communications in criminal investigations : "*(i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed.*"[1]

In cases concerning national security, although the Court recognized that "*national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security*"[2], it has considered that "***the same six minimum safeguards also apply in cases where the interception was for reasons of national security***"[3]. It has added, in such national security cases, **three additional safeguards** that must be met, "*in view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them*"[4] : the Court "***also has regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law***."[5]

The points below will demonstrate that **these nine safeguards demanded by the ECtHR, that are minimal safeguards, do not exist, or are severely insufficient, in Greek law**, in particular the guarantees concerning the procedures for authorizing surveillance, the foreseeability of the grounds for authorizing it, the existence of remedies, as well as the nature, scope and duration of the surveillance.

Reporters Without Borders (RSF) calls on Greek authorities to provide for such guarantees in the law in order for its legal framework on the right to privacy and on journalistic freedoms to meet international standards of Human Rights.

---

[1] ECtHR, Big Brother Watch and others v. the United Kingdom, 2021, § 335 - https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}

[2] *ibid*, § 338

[3] *ibid* - emphasis added

[4] *ibid*, § 339

[5] *ibid*, § 338 - emphasis added

1. Lack of judicial oversight in cases of surveillance operated on national security grounds

● Lack of independent judicial authorisation

In cases *not* involving national security, requests by security services to breach the confidentiality of an individual's communication are to be accepted by a panel of three judges.

The procedure is completely different in cases where a threat to national security is alleged : the request by security services to breach the confidentiality of an individual's communication is not submitted to a judge, but to a special prosecutor, who cannot be regarded as an independent judicial authority.

Although a recent law has been adopted that provides that now two prosecutors, instead of one, must authorize surveillance, this remains insufficient.

This special procedure applicable in cases of national security contradicts the safeguards the ECtHR considers should be applied. The Court has indeed ruled that :

> *In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole (...)* ***it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure****.*[6]

In another judgment, the court has considered that the fact that relevant authorities must seek judicial authorisation for the surveillance "*is an important safeguard against arbitrariness and abuse*", as it "*can limit their discretion in interpreting that notion* (of national security) *and ensure that sufficient reasons to place someone under surveillance are present in each case*"[7]

⇒ Greek legislation should allow for an independent judicial overview of requests for surveillance by security services, and for an independent judicial authority to authorize such requests, including in cases where a breach of national security is alleged.

⇒ Greek law should also oblige security forces to justify the request for surveillance, in order for judicial review to assess whether it complies with the principles of legality, necessity and proportionality.

● Impossibility of effective oversight of the necessity and proportionality of the surveillance

When surveillance of an individual is requested on grounds of national security, the request to the prosecutor need not specify the grounds and motives of the surveillance, making it impossible for the prosecutor to assess whether the requested surveillance meet the requirements of necessity and proportionality, and to assess whether the surveillance shall continue or be ended.

This directly contradicts the ECtHR case law according to which surveillance must meet the principles of necessity and proportionality. The Court indeed holds that

[6] *ibid*, § 336

[7] ECtHR, Ekimdzhiev and others v. Bulgaria, 2022, § 301 - https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-214673%22]} - emphasis added

> *In order to provide an effective safeguard against abuse, the independent authorising body should be i**nformed of both the purpose of the interception** and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.*[8]

⇒ Greek legislation should ensure not only the independence, but also the effectivity, of the oversight of the necessity and proportionality of the requested surveillance

- ## Absence of judicial review once the surveillance is terminated ; violation of the right to effective remedy

After the Koukakis case, Greek law was reviewed in a way that it no longer provides for any possibility for the individuals affected by surveillance to be informed of the said surveillance after it ended, even in cases where the surveillance did not confirm the suspicion of breach to national security.

It should be noted that before the recent amendment, it was provided that the Hellenic Authority for Communication Security and Privacy (ADAE) could notify the aggrieved person of the lifting of the surveillance, whether it was for the investigation of serious crimes or for reasons of national security.

This makes it impossible for a judicial review to be operated on the surveillance, to ensure it complies with the requirements of legality and necessity. The ECtHR has however considered that "*review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated.*"[9] As regards the third stage, after the surveillance has been terminated, the Court holds that :

> *The question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers.*[10]

This recent amendment to the law therefore violates the right to an effective remedy to be exercised against abusive surveillance.

⇒ Greek authorities should repeal, with retroactive effect, the recent amendment to the law that prevents individuals from being informed of the fact they were submitted to surveillance, to ensure they can exercise their right to effective remedy.

[8] ECtHR, Big Brother Watch and others v. the United Kingdom, 2021, *op. cit.*, §352
[9] *ibid*, § 336
[10] *ibid*, § 337

2. Lack of safeguards against abuse of surveillance

● Lack of limitation of the period of surveillance

Article 5 of Law 2225/1994 does not provide any maximum period during which surveillance may be performed in cases of national security - unlike in cases concerning investigation of offenses, where the maximum limit is 10 months.

The absence of limitation violates the case law of the ECtHR. The Court, in a judgment referring to the 2-year maximum limit for surveillance provided for in Bulgarian law, expressed the view that "*the sheer length of that period, coupled with the inherently unclear contours of the notion of national security, significantly weakens the judicial control to which such surveillance must be subjected.*"[11]

This is *a fortiori* the case in Greece where no time limitation is provided for in cases of national security.

⇒ Greek legislation should provide for a proportionate limitation of the period during which an individual can be placed under surveillance on grounds of national security, in line with the case law of the ECtHR.

● Lack of specifications of the types of communications that may be intercepted of the means of interceptions

The Greek legislation on the secret surveillance of citizens for national security reasons does not specify the types of communication for which the lifting of secrecy may be requested, such as IP addresses, or electronic communications. Article 5-1 of Law No 2225/1994 merely states that interception orders must specify the types of communications that can be intercepted, leaving the ordering authority complete latitude to decide to intercept any type of communications without limitation.

The law does not specify either the means by which interception may be requested.

This lack of specifications gives too broad a power to security forces and violates the principles of necessity and proportionality demanded by the European Convention.

⇒ The law should limit by law the types of communications that may be intercepted and the means by which the interception may be performed.

● Lack of limitation of information that may be collected

In the case of Stavros Malichudis, it has been revealed that information collected about him did not concern any breach of the law, but related to his political affiliations, journalistic activities, etc.

This confirms that the lack of judicial oversight and sufficient limitations in the law make it possible to perform abusive surveillance, in violation of the principle of "*necessity in a democratic society*" provided for by the ECtHR.

[11] ECtHR, Ekimdzhiev and others v. Bulgaria, 2022, *op. cit.*, § 305

⇒ The law should ensure that information collected are only those relevant to an alleged perpetration or preparation of a crime.

● Absence of provision providing for the destruction of collected data

Article 5 of Law 2225/1994 does not include any procedure for the destruction of data collected under a national security procedure in cases where investigations have not confirmed the suspicions of breach of national security - unlike in the case of investigations not concerning national security, where the data in question are destroyed if they do not constitute evidence.

The law does not provide either for any competent authority to take charge of the storage and preservation of these records.

⇒ The law should provide for a procedure of destruction of data collected when investigations on alleged breaches of national security did not confirm such allegations ;

⇒ Such procedure should be performed under the control of an independent authority or a judicial authority ;

⇒ Individuals should have the right to be informed of such destruction, and to appeal to a judge to ensure destruction was performed.

3. Lack of specific safeguards against surveillance of journalists

Given their social function to inform the public on issues of public interest and to monitor the actions of public authorities, journalists must benefit from specific rights, in particular the right to protect the confidentiality of their sources. In that regard, the ECtHR has repeatedly judged that

> *The safeguards to be afforded to the press are of particular importance, and the protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be affected adversely*.[12]

Surveillance of journalists is particularly concerning as it may "*have a detrimental impact, not only on the source, 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 by the disclosure; and on members of the public, who have an interest in receiving information imparted through anonymous sources*".[13]

Surveillance of journalists is by nature likely to violate the confidentiality of their sources. The Court therefore considers that

[12] ECtHR, *Goodwin v. the United Kingdom,* 1996, § 39 - https://hudoc.echr.coe.int/eng#{%22appno%22:[%2217488/90%22],%22itemid%22:[%22001-57974%22]}

[13] ECtHR, Big Brother Watch and others v. the United Kingdom, 2021, *op. cit.*, § 443

> ***Any interference with the right to protection of journalistic sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake.*** *First and foremost among these safeguards is the* ***guarantee of review by a judge or other independent and impartial decision-making body*** *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.*
>
> *Given the preventive nature of such review the judge or other independent and impartial body must be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be assessed properly. The decision to be taken should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of journalist's source*[14]

This ruling clearly strengthens RSF's argument that surveillance, even in national security cases, must be subjected to prior and continued independent judicial review. Such oversight should be strengthened in cases involving a journalist.

⇒ The law should provide for specific guarantees in cases where surveillance is requested against a journalist. Such guarantees should provide in particular :

- **the requesting authority obligation to demonstrate that surveillance does not aim at identifying the journalists' sources, unless it demonstrates their exists an overriding requirement in the public interest in accordance with the ECtHR case law ;**
- **independent judicial overview is strengthened and continued in surveillance involving a journalist ;**
- **where surveillance of a journalist is authorized by an independent judicial authority, that authority must ensure that the surveillance and the data collected are strictly limited to the motives of the authorisation and does not spill over unrelated information, in particular information related to the journalistic activity or the confidentiality of sources**
- **indirect or incidental surveillance of a journalist (where the journalist is not him or herself the target of the surveillance, but is in contact with a person who is the direct target of the surveillance) should immediately necessitate a specific judicial control and authorisation, in order to ensure confidential information related to the journalist's activity or his sources are not collected.**

[14] *ibid*, § 444 and 445 - emphasis added

4. Lack of sufficient legal framework on the use of spyware

The Koukakis case has revealed that the Predator spyware was used against the journalist - even though the use of spyware is not provided for by the law and is therefore illegal.

The use of spyware - although it may be an effective tool to fight for instance against organized crime, drug trafficking or terrorism - make it possible to severely violate the right to privacy and journalists rights. It must therefore be explicitly provided and strictly regulated by the law.

The guarantees existing in Greek law against the use of such technological tools are too weak. For instance, and as stated above, Greek legislation does not specify the means by which surveillance may be performed, allowing the authorities to use any means they deem necessary, however disproportionate it may be.

⇒ The Greek legislation should make it mandatory for the executive authorities to reveal and discuss publicly the use of such spywares, the buying of such spyware or the use of intermediaries to perform surveillance through the use of such spyware.

⇒ The law should make it clear that where surveillance is not possible under the law, the use of spyware is not possible either.

⇒ The same requirements as stated in this document (necessity, proportionality, independent judicial oversight, limitations, etc.) should apply whether surveillance is performed using spywares, including by intermediaries.

⇒ The same guarantees concerning journalists should apply where surveillance is performed by spywares.

5. Vague definition of national security

Threats to national security make it possible to breach the confidentiality of communications according to Greek law - and as provided for by international standards and the European Convention of Human Rights (article 8). However the law does not provide for any definition of “national security” or “breach of national security”. Articles 3 and 5 of Law No 2225/1994 which set the procedure for lifting confidentiality on grounds of national security make no mention of the categories of people who may be considered a threat to national security and allow to breach the confidentiality of communication of any citizen, and do not provide for any procedure to challenge the breach.

This lack of definition and clarity contradict the case law of the European Court of Human Rights (ECtHR), which states that any interference with an individual’s right to privacy can only be justified if it is in accordance with the law, pursues a legitimate aim according to article 8-2 of the convention (among which national security) and is necessary in a democratic society in order to achieve any such aim. The Court has emphasized that the law allowing such interference must be “**foreseeable**” :

> *The meaning of “foreseeability” in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, “foreseeability” cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly.* ***However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident****. It is therefore essential to have clear, detailed rules on secret surveillance measures (...)* ***The 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.***[15]

The condition of foreseeability cannot be regarded as being met when the grounds allowing for a breach of the confidentiality of communications of an individual are insufficiently defined.

⇒ Greek authorities should review the legislation on national security, to ensure that the conditions allowing for surveillance on its ground meet the requirements of legitimacy, necessity and foreseeability.

⇒ At the minimum, the legislation should define what constitutes a breach to national security, and provide for a definition of the categories of people that may be considered a threat to national security, and the objects which may be placed under surveillance.

For more information :
Paul Coppin, Assistant to the Director of Advocacy, Head of the Legal Desk
at Reporters Without Borders
paul.coppin@rsf.org

[15] *ibid*, § 333 - emphasis added.