



**Greek National Commission for Human Rights**

**Reference Report  
on the institutional framework for the oversight of  
security and intelligence services**

**2023**



*The Greek National Commission for Human Rights (GNCHR) is the independent advisory body to the Greek State and the national institution for the protection and promotion of human rights (NHRI) in Greece. It was established by Law 2667/1998 in accordance with the UN Paris Principles. The founding legislation of the GNCHR was amended by Law 4780/2021, the provisions of which now govern its operation. Its Plenary Assembly is composed of persons designated by twenty institutions (independent authorities, trade unions, human rights organisations, higher education and research institutions)*

---

Neofytou Vamva 6, 106 74 Athens

T: 210 72 33 221-2, W: [www.nchr.gr](http://www.nchr.gr), E: [info@nchr.gr](mailto:info@nchr.gr)



## Reference Report on the institutional framework for the oversight of security and intelligence services

### Table of contents

Greek National Commission for Human Rights.....	1
Reference Report on the institutional framework for the oversight of security and intelligence services .....	3
PRELIMINARY OBSERVATIONS* .....	6
i) The role and mission of the GNCHR.....	6
(ii) Purpose of the present Report.....	8
B. Protection of the rights of confidentiality of communications.....	9
1. The scope and historical roots of the right.....	9
2. Constitutional protection .....	11
2.1 The meaning of the term “confidentiality” .....	11
2.2 Clarifying the meaning of terms: “secrecy – intimacy – privacy” .....	12
2.3 The status mixtus of the right and how it is related to other fundamental rights .....	13
3. Restrictions on the confidentiality of communications (Article 19(1) (b) of the Constitution .....	14
3.1 Lifting of confidentiality for national security purposes.....	15
3.1.1 Who is to authorise the lifting of confidentiality .....	16
3.1.2 The waiver of confidentiality procedure.....	18
3.1.3 Defining the concept of “national security” .....	19
3.1.4 Lifting of communications confidentiality of political figures .....	21
4. The establishment of an independent authority for the protection of communications .....	23
4.1 Constitutional provisions for the independent authorities (Article 101A of the Constitution) .....	23



4.2 Legislative and institutional framework of operation of the Hellenic Authority for Communication Security and Privacy (ADAE) .....	24
4.3 Constitutional obligations to be fulfilled by independent authorities and the ADAE, as set out by the common legislator .....	28
C. Confidentiality of communications in other legal orders .....	29
1. Comparative overview within the European Union .....	30
1.1 Comparative review of the lifting of confidentiality purposes .....	31
1.2 Intelligence services oversight bodies.....	32
1.3 Oversight delimitation and exercise of powers of control over intelligence services.....	33
1.4 Effective legal remedies for persons affected.....	36
D. Concluding Observations.....	37





## PRELIMINARY OBSERVATIONS\*

### i) The role and mission of the GNCHR

The [Greek National Commission for Human Rights](#) (GNCHR), is **the independent advisory body to the Greek State** in the field of human rights protection and **the National Human Rights Institution** (NHRI) in Greece, established by [Law 2667/1998](#) in accordance with [the UN Paris Principles](#) adopted by [the United Nations \(General Assembly Resolution A/RES/48/134, 20.12.1993, “National institutions for the promotion and protection of human rights” \(NHRIS\)\)](#) Its founding legislation was amended by [Law 4780/2021](#), the provisions of which now govern the operation of the National Commission. Under the provisions of [Law 4780/2021](#) the GNCHR has acquired legal personality, operational and financial independence and administrative autonomy. Since 2001, the GNCHR has been recognised as fully compliant with the Paris principles and has an A Status accreditation, indicative of its independence and effective fulfilment of its role.

According to its founding law, the main mission of GNCHR consists of:

- constantly **monitoring** matters pertaining to human rights protection,
- informing the public and advancing research in this connection
- **exchanging experience** at international level with the competent institutions, such as the United Nations Organisation, the Council of Europe, the OSCE, other NHRIS, as well as with Civil Society organisations and
- the formulation of policy proposals on matters related to its scope of work

In particular, in the context of its mission, the GNCHR has the competence to **continuously point out to all State institutions** the need for effective protection of human rights, to inform public opinion about the relevant risks of violation and, **above all, to provide advice to the Greek State** on the development of a proper central policy on issues related to human rights.

An additional guarantee of the GNCHR independence is its **pluralistic and polyphonic composition** which allows it to foster a unique dialogue between the various bodies of Civil Society and the State. Its **Plenary is composed by 20 members**, designated by NGOs, trade unions, Independent Authorities, Universities and Bar Associations. About 30 **representatives of the political parties, the Parliament and Administration, in total, participate in the Commission as liaison officers**. An equal number of alternates are appointed for both members and liaison officers.

Moreover, the GNCHR contributes with Observations to the Reports submitted by Greece during the periodic review of our country's compliance with the international



commitments it has undertaken upon ratification of international human rights instruments, while in parallel it **submits its own independent Reports**. In practice, in the context of its institutional role and mission as a guardian of human rights at international, regional and national level, the GNCHR plays a central role in **bridging the gap** not only between the State and Civil Society, but also between the Country's international commitments to the implementation of human rights and their real enjoyment in practice.

The National Commission, in the context of its dual role, as the independent advisory body to the Greek State and the National Human Rights Institution in Greece, **is monitoring the issue that has become the subject of public debate** on the surveillance of public and private figures, by attributing the utmost importance to safeguarding the right to confidentiality of communications. The Commission reiterates that it has previously given its views on the confidentiality of communications and the protection of personal data and has expressed its deep concern about regulations that remove or restrict privacy and make individuals or groups targets of surveillance. Besides, the National Commission **has focused on recent legislative developments on confidentiality of communications, cybersecurity and protection of personal data** and has expressed its reservations about them.

\* This text was adopted by the Plenary of the GNCHR on 02.03.2023. Rapporteurs, Professor Maria Gavouneli, President of the GNCHR, Giannis Ioannidis, First Vice - President of the GNCHR, Ioanna Pervou, Adjunct Lecturer, Faculty of Law, Democritus University of Thrace - (D.U.Th.) and Dr Anastasia Chalkia, Human Rights Officer, Member of the Scientific Staff of the GNCHR. Thanks for their contribution to Professor Nikolaos Livos (Alt.Member of the Hellenic Data Protection Authority) and to Ekaterina Papanikolaou, PhD (Member of the Hellenic Authority for Communication Security and Privacy (ADAE)).



## (ii) Purpose of the present Report

During the second half of 2022, public debate was focused on the surveillance of journalists, politicians and high-ranking officers of the Greek Army through specific surveillance software. The (illegal) use of ‘spyware’ for surveillance purposes by states poses a threat to human rights, democracy and the rule of law.

On 10 March 2022, the European Parliament decided to set up the PEGA committee to investigate alleged infringements and maladministration in application of EU law in relation to the use of ‘Pegasus’ and equivalent spyware surveillance software. In particular, the PEGA Committee is called upon to collect information on Member States or third countries that engage in surveillance of citizens and violate the rights and freedoms enshrined in the EU Charter of Fundamental Rights. In parallel, a committee of inquiry was set up in the Greek Parliament, but the outcome of the process was classified as confidential. Similarly, the discussion at the meeting of the Special Permanent Committee on Institutions and Transparency, as provided for in Article 43(A) of the Standing Orders of the Hellenic Parliament was classified as confidential.

Later, on 29 November 2022, a Bill was submitted to the Parliament by the Ministry of Justice on "Lifting of the confidentiality of communications, cybersecurity and the protection of citizens' personal data (subsequent Law 5002/2022), at the discussion stage of which, the GNCHR submitted a **Note** expressing its serious reservations on the proposed regulations. In January 2023, the Public Prosecutor at the Greek Supreme Court (*Areios Pagos*) issued a report interpreting provisions of Law 5002/2022 at the request of a telecommunications company.

Surveillance of individuals, results in serious infringements of fundamental rights, while the increasing use of technology has made surveillance tools much easier and user-friendly than they used to be. For this reason, the **Venice Commission** at its 106 plenary session (Venice 11-12 March 2016) made a special reference to the collection of data and surveillance when assessing the level of compliance with the Rule of Law in a given State. In particular for *targeted* surveillance, namely, “*covert collection of conversations by technical means (bugging), covert collection of the content of telecommunications and covert collection of metadata*” <sup>1</sup>, the

---

<sup>1</sup> According to the Venice Commission, “The level of the interference metadata collection involves in private life is disputed. The CJEU has extended privacy protection to metadata as well. The case law of the ECtHR so far accepts that lesser safeguards can apply for less serious interferences with private life. [...]. Where no prior judicial authorisation is provided for metadata collection, there must at least be

Venice Commission sets out the following **criteria to provide guarantees against abuse of power in cases of targeted surveillance:**

- i) Is there a mandate in the primary legislation and is it restricted by principles like the principle of proportionality?
- ii) Are there norms providing for procedural controls and oversight?
- iii) Is an authorisation by a judge or an independent body required?
- iv) Are there sufficient legal remedies available for an alleged violation of individual rights?<sup>2</sup>

In view of all the above, the GNCHR decided to draw up a Reference Report on the institutional framework for the control of security and intelligence services, which was announced in the the Press Release of 23.01.2023. The role of security and intelligence services in the fight against crime and the protection of national security is crucial. On the other hand, their work interferes with the enjoyment of human rights and places restrictions on ensuring the confidentiality of communications and the protection of personal data, which are two pillars of the rule of law.

The question that arises, taking into account what has taken place in Greece over the last six months, is how authorities can use data and technology to fight against crime and protect national security, so that fundamental rights enshrined in international and national law, such as the right to family life, the right to privacy, the freedom of thought, the freedom of opinion and expression, personal data and confidentiality of communications, are fully respected. In the light of the above, the issue of oversight and control of intelligence services, i.e. their accountability to independent authorities, the judiciary and the executive, becomes of major importance.

## **B. Protection of the rights of confidentiality of communications**

### **1. The scope and historical roots of the right**

The confidentiality of communications constitutes a specific, autonomous fundamental right<sup>3</sup> that is enshrined as an independent constitutional right in several legal orders

---

strong independent post hoc review.”: Council of Europe, ‘The rule of law checklist’, Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016), Athens: Hellenic Parliament, 2022, p.104.

<sup>2</sup> See: Articles 8 and 13 of the ECHR.

<sup>3</sup> Nikolaos Papadopoulos, ‘Article 19’ in F. Spyropoulos et al., *The Constitution of Greece, Article by article interpretation* (Sakkoulas Publications: Athens – Thessaloniki, 2017) 469-494, 481; Fereniki Panagopoulou, Article 19: Secrecy of letters, correspondence and confidentiality of communications’ in



and<sup>4</sup> protected internationally.<sup>5</sup> The protection of communications in most legal orders represents a more specific aspect of the protection of privacy.<sup>6</sup> The protection of the confidentiality of communications is a cornerstone of the democratic state organisation and the rule of law, which is confirmed by the historic nature of this right.<sup>7</sup> More specifically, despite the inherently narrow scope of the definition of the secrecy of letters, correspondence and confidentiality of communications, the protection of the right has over time been of major importance in the course of the constitutional development of many countries. It has become a key criterion for the quality of protection of individual freedoms, as it epitomises the essential distinction between private and public life.<sup>8</sup>

In summary, the evolution of the freedom of communication is in line with technological developments and the institutional framework for the protection of the right to confidentiality of communications, has been broadened over four stages.<sup>9</sup> In the first place, the protection of confidentiality applied to certain forms of communication, such as letters (a), while at a later stage it also covered all forms of indirect communication (correspondence) (b). Subsequently, the confidentiality of communications was deemed to cover all forms of direct and indirect communication

---

SP. Vlachopoulos, X. Kontiadis, G. Tasopoulos (ed.) *The Constitution of Greece, Article by Article interpretation* (electronic version) <<https://www.syntagmawatch.gr/my-constitution/arthro-19/>> last accessed on 3 February 2023.

<sup>4</sup> Article 19 (1) of the Basic Law for the Federal Republic of Germany provides that “The privacy of correspondence, posts and telecommunications shall be inviolable”. Article 15 of the Constitution of the Italian Republic respectively, provides that, “Freedom and confidentiality of correspondence and of every other form of communication is inviolable.”

<sup>5</sup> Article 17 (1) of the ICCPR provides that, “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.” Similarly, pursuant to 8 (1) of the ECHR stipulates that, “Everyone has the right to respect for his private and family life, his home and his correspondence”. See also Article 7 of the CFREU according to which “Everyone has the right to respect for his or her private and family life, home and communications.”

<sup>6</sup> See, for example, Spanish Constitution Article 18 (3), which stipulates that the right to confidentiality of communications, constitutes a specific aspect of privacy and provides that “Secrecy of communications is guaranteed, particularly regarding postal, telegraphic and telephonic communications, except in the event of a court order”.

<sup>7</sup> See *Prince Albert v. Strange*, England and Wales High Court (Chancery Division) Feb 8, 1849. This is one of the first cases before the English courts regarding the illegal possession and publication of engravings by Prince Albert.

<sup>8</sup> Judith Wagner Decew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Cornell University Press: Ithaca, 1997) 9-10.

<sup>9</sup> Lisl Brunner, ‘Digital Communications and the Evolving Right to Privacy’ in Molly K. Land & Jay D. Aronson (edit.) *New technologies for Human Rights Law and Practice* (CUP: Cambridge, 2018) 217-242, 221.

(c), and now, as a further safeguard to ensure the most effective protection, an additional set of guarantees was introduced (d).<sup>10</sup>

## 2. Constitutional protection

In the Greek legal order, the protection of the secrecy of communications is provided for in Article 19 of the Constitution, as revised in 2001. The choice of the law maker to protect this right independently, indicates the importance attached to it by the Greek legal order.

### 2.1 The meaning of the term “confidentiality”

The term "confidentiality" reflects the safeguard of secrecy of communication, when there is both the subjective expectation of the participants to this effect and the objective social judgement that the communication is reasonably private. In other words, there is a 'reasonable expectation of privacy' within and outside the context of communication.<sup>11</sup> The co-existence of the two elements is widely accepted to constitute a *minimum* for the protection of the confidentiality of communications, as it has been articulated and developed *grosso modo* in the jurisprudence of several legal orders<sup>12</sup> and accepted in its essence by the ECtHR.<sup>13</sup>

In the Greek legal order, where there is a reasonable expectation of privacy, body of theory and case law suggest that communication *per se* is protected, with differentiations in terms of its external details. The confidentiality of communications covers any type of communication (letters, free response, communication), and an increasingly wide range of details and data, provided that there is a reasonable expectation of privacy.<sup>14</sup> It should be noted, however, that although "external details" constitute an integral part of the confidentiality of communications, they are not related to privacy and they are therefore protected even when they are not "private". Apart from the message of the communication, both external details and traffic, location or geolocation data are protected. Overall, the list of details covered by confidentiality

---

<sup>10</sup> Papadopoulos (2017) 473.

<sup>11</sup> Samantha Arrington, 'Expansion of the Katz Reasonable Expectation Privacy Test Is Necessary to Perpetuate a Majoritarian View of the Reasonable Expectation of Privacy in Electronic Communications to Third Parties' (2013) 90 2 UDetMercyLRev 179-202, 182-183; Eric Barendt, 'Problems with the 'reasonable expectation of privacy' test' (2016) 8 2 JMediaL 129-137, 133.

<sup>12</sup> *Katz v. United States*, 389 US 347, 361 (Judge Harlan concurring); *Kinloch v. Her Majesty's Advocate* [2012] UKSC 62.

<sup>13</sup> *NUH Uzum et al v. Turkey*, App. nos 49341/18 and others (ECtHR 29 March 2022) §§53-70; *LL v. France*, App. no 7508/02 (ECtHR 10 October 2006) §46; *Erdem v. Germany*, App. no 38321/97 (ECtHR 5 July 2001); *Klass et al v. Germany*, App. no 5029/71 (ECtHR 6 September 1978)

<sup>14</sup> See, for example, Hellenic Council of State 1593/16, Judgement of the Supreme Court Plenary Session 1/17, Opinion of the Public Prosecutor at the Greek Supreme Court (*Areios Pagos*) 9/2011,



grows depending on the details that are detectable and leave a trace.<sup>15</sup> In summary, the details or data protected by the Constitution relate to both the external and internal elements of the communication, the latter being further subdivided into principal and connecting, which are equally protected.<sup>16</sup>

Given its outstanding importance, the protection of confidentiality of communications is therefore enhanced in many ways. Therefore, in case it is not immediately obvious whether a communication is confidential, it will be presumed to be so in accordance with the principle in *dubio pro libertate*.<sup>17</sup> This is a necessary interpretative choice of the above in order to meet the high threshold set by the Hellenic Constitution that the secrecy of communications is "absolutely inviolable".<sup>18</sup>

## 2.2 Clarifying the meaning of terms: "secrecy – intimacy – privacy"

Apart from clarifying the meaning of the terms contained in Article. 19 (1)(a) of the Constitution, of particular interest is the *ratio* of the protection of the confidentiality of communications. There is a plurality in theory regarding the constitutional establishment of the confidentiality of communications as an independent right. It is argued that the protection of confidentiality derives from the secrecy that the right holders wish to confer on their communications or responses.<sup>19</sup> While this was initially a tautological position, since confidentiality and secrecy were considered to be identical, now this view is being reversed, as it is possible to breach the confidentiality even in a communication that is public and not secret. Thus, the term secrecy is likely to be confusing, as it also refers to the safeguarding of information when confidentiality is lifted for national security purposes and reasons relating to public interest. Consequently, secrecy is more of a principle concerning disclosure of information in exceptional cases of lifting the confidentiality of communications and less of a justificatory basis for the right itself.<sup>20</sup>

---

<sup>15</sup> Arianna Vedaschi & Valerio Lubello, 'Data Retention and Its Implications for the Fundamental Right to Privacy' (2015) 20 1 TilburgLRev 14-34, 21.

<sup>16</sup> Nikolaos Livos, 'The criminal protection of the telecommunications connecting data' (1997) MZ Criminal Chronicles 737-759, 737.

<sup>17</sup> Konstantina Arkouli, *Protection of Personal Data in Electronic Services* (Nomiki Bibliothiki: Athens, 2010) 61.

<sup>18</sup> Stavros Tsakyrakis, 'The confidentiality of communications: Absolutely inviolable or a wish of the legal order?' (1993) 41 NoB 995 et seq.; George Kaminis, 'The confidentiality of telephone communication: Constitutional protection and its implementation by the criminal legislator and the courts' (1995) 43 NoB, 445 et seq.

<sup>19</sup> Papadopoulos (2017) 477.

<sup>20</sup> Yannis A. Tassopoulos, 'The Hollow Core of the Right to Confidentiality of Communications and National Security' (2022) 3 e-Politeia 340-359, 347.

On the other hand, it is argued that the *raison d'être* of the right is the protection of two or more persons in intimacy, in the light of the fact that intimacy qualitatively differentiates communication from any form of public expression.<sup>21</sup> Although the above position reflects the distinction between public and private communications, intimacy significantly limits the scope of the confidentiality of communications. Even in this case, the above theoretical approach is not absolute, since the confidentiality of means constituting a communication is protected, even if it is deemed to be public (notably with regard to its metadata - cf. ECtHR, *L.B. v. Hungary* 36345/16).

According to international standards, confidentiality of communications constitutes a specific part of one's privacy and a necessity for the respect of the right to private life.<sup>22</sup>

### **2.3 The status mixtus of the right and how it is related to other fundamental rights**

The above mentioned indicate the legislative proximity of the confidentiality of communications with the protection of private life, the protection of personal data and the freedom of expression (Articles 9, 9 (A) and 14 (1) of the Constitution respectively). More specifically, freedom of expression safeguards the possibility of "communicating", which is a necessary condition for the protection of its confidential nature.<sup>23</sup> Furthermore, as mentioned above, the confidentiality of communications is better safeguarded if considered as a more specific aspect of one's private life. Finally, technological developments and the now preferred forms of communication show that the protection of confidentiality implies protecting also personal data, or, on the contrary, that the breach of the confidentiality of communications mostly implies an infringement of Article 9 (A) of the Constitution.<sup>24</sup> Consequently, there is a comprehensive and complete constitutional protection framework, from which the intrinsic connection between confidentiality of communications and respect for freedom of expression and privacy arises. Already in the VIIth Revisionary Parliament, the majority rapporteur pointed out that privacy does not only concern the classic right to confidentiality of communications, but also depends on the right to private and family life (Article 9 of the Constitution) and the prohibition of unlawful collection and

---

<sup>21</sup> Kostas C. Chrisogonos, *Individual and Social Rights* (Athens: Nomiki Bibliothiki, 2006) 257.

<sup>22</sup> UN Human Rights Committee (HRC), 'CCPR General Comment No. 16. Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation', 8 April 1988, §8.

<sup>23</sup> Nikolaos Papadopoulos, 'Article 14' in F. Spyropoulos et al., *The Constitution of Greece, Article by article interpretation* (Sakkoulas Publications: Athens – Thessaloniki, 2017) 309-355, 318.

<sup>24</sup> Linos-Alexandros Sicilianos, *European Convention on Human Rights, Article by article interpretation* (Athens: Nomiki Bibliothiki, 2013) 327- 328.

processing of personal data (Article 9 of the Constitution), thus raising the revisionary challenge for a unified constitutional provision.<sup>25</sup>

Finally, although the confidentiality of communications is primarily an individual freedom, as it enshrines a *status negativus* for the holders of the right, increased positive obligations have been established for the State to safeguard it (*status positivus*), while the possible violation of the right on a large scale constitutes a direct threat to the State organisation (*status activus*). The positive dimension of the right follows directly from the literal interpretation of Article 19 of the Constitution, since the constitutional legislator provides for a complete legal framework on the protection of the right, enhanced constitutional guarantees. As far as the political dimension of this right is concerned, it is recognised as *a sine qua non* of a State subject to the rule of law, which is placed at the core of the State organisation.<sup>26</sup>

### **3. Restrictions on the confidentiality of communications (Article 19 (1)(b) of the Constitution**

Although Article 19 (1)(a) of the Constitution provides that the secrecy of communications is absolutely inviolable, a special reservation of law is introduced in the second subparagraph, by the constitutional legislator. In particular, four specific conditions are set which must be satisfied simultaneously for the release of confidentiality: a) the existence of primary legislation or a regulatory act following<sup>27</sup> a legislative delegation, b) the existence of guarantees ensuring that the waiver of confidentiality is allowed exceptionally, so as not to circumvent the core of the right, c) the waiver is carried out by the judicial authority, and (d) it is enforced either for national security purposes or for the detection of particularly serious crimes.

It follows readily that the constitutional legislator has set a particularly strict framework under which the confidentiality of communications is lifted. Furthermore, since the lifting of confidentiality is the exception to the rule, the above conditions must be interpreted restrictively. The basic criterion in both categories of cases of lifting of confidentiality is to strike a balance between the protection of the right and the safeguarding of public order, both for national security purposes and for the detection

---

<sup>25</sup> VIIth Revisionary Parliament Period I' - Session A' Constitutional Revision Committee, General Rapporteur of the Majority Evangelos Venizelos (Athens, October 2000) <<https://www.evenizelos.gr/images/stories/e-books/EVenizelos-EisigisiAntheorisiSyntagmatos2000.pdf>> last access 3 February 2023, 19.

<sup>26</sup> Aikaterina A. Papanikolaou, 'Restrictions on the Right to Free, Confidential Communication: Actual Thoughts on a Timeless Dilemma' (2020) constitutionalism <<https://www.constitutionalism.gr/wp-content/uploads/2020/07/2020-07-papanikolaou-katerina-aporrto-epikoinonias.pdf>> last accessed February 3, 2023, 2.

<sup>27</sup> See Legislative Act of 9.8.2022 (Official Government Gazette A' 152/9.8.2022) 'Urgent provisions to enhance integrity in the operation of the National Intelligence Service', No 2.



of crimes. As regards the detection of particularly serious crimes, the common legislator does not allow a wide margin of interpretation, as these are criminal offences exhaustively listed in the implementing legislation of Article 19 of the Constitution.

Therefore, in these cases of lifting of confidentiality there is a clear and relatively well-established legal framework.<sup>28</sup> However, the same does not apply to the lifting of confidentiality for reasons of national security.

### 3.1 Lifting of confidentiality for national security purposes

With regard to common legislation, the triptych of Articles 19 (1), 9 and 9A of the Constitution has led to a multitude of laws, which in turn does not strengthen the protection of confidentiality. In particular, apart from the implementing Law 2225/94<sup>29</sup>, as amended by Law 5002/22<sup>30</sup>, referred to in Article 19 of the Constitution, a complex legislative framework is in place.<sup>31</sup>

---

<sup>28</sup> See comparatively the provision no. 4 (3) of Law 2225/94 as amended by Article 6 of law 5002/22. The safeguard for non-abusive lifting of confidentiality in cases of detection of particularly serious crimes is ensured mainly by the strictly standardised nature of the criminal phenomenon. Thus, despite the fact that the list of crimes, the detection of which may give rise to a request for the lifting of the confidentiality of communications, has been considerably extended in recent years, it is assumed that the relevant legislative provisions aim at suppressing and preventing criminal acts. Furthermore, safeguards for the lifting of confidentiality that are universally considered to be adequate include the legislative provision that the relevant decision must be taken, respectively, by the Judicial Council of the Court of Appeals or the Plenary Courts, as the Council with territorial and substantive jurisdiction. Furthermore, even before the entry into force of Law 5002/2022, it was established theoretically and jurisprudentially that the constitutional provision on 'particularly serious crimes' does not only apply to felonies, but also to misdemeanours. The above helped to consider the legislative framework complete and comprehensive. Certainly, the key element to ensure that lifting of confidentiality is not unfairly used, is the exhaustive list of criminal offences. On the contrary, legislative references to categories of criminal acts inevitably give rise to concern. Aikaterina Papanikolaou, 'Concern over the new lifting of confidentiality rules' (16 December 2019)' (16 December 2019) Ta Nea <<https://www.tanea.gr/print/2019/12/16/economy/anisixia-apo-to-neo-kathestos-arsis-tou-aporritou/>> last accessed 3 February 2023: see also Law 4640/2019 (Official Government Gazette A' 190/30-11-2019) which extended the list of offenses justifying the lifting of confidentiality.

<sup>29</sup> Law 2225/1994 ('Official Government Gazette A' 121/20.07.1994) "On the protection of the freedom of response and communication and other provisions".

<sup>30</sup> Law 5002/2022 (Official Government Gazette A' 228/09.12.2022) "Procedure for the lifting of the confidentiality of communications, cybersecurity and protection of personal data of citizens".

<sup>31</sup> The legislative framework is mainly summarised in the following legal instruments, Law 3471/2006 (Official Government Gazette A' 133/28.06.2006) "Protection of personal data and privacy in the field of electronic communications and amendment of Law 2472/1997": Law 3674/2008 (Official Government Gazette A' 135/10.07.2008) "Strengthening the institutional framework for safeguarding the confidentiality of telephone communications and other provisions": Presidential Decree 47/2005 (Official Government Gazette A' 64/10.03.2005) "Procedures and technical guarantees for the lifting of and ensuring the confidentiality of communications", while dispersed provisions are also found in Law 3115/2005 (Official Government Gazette A' 47/27.02.2003) "Hellenic Authority for Communication

The key points at the core of the legislative change of Law 5002/22 relate to the lifting of confidentiality for national security purposes: 1) who is to give the order to lift the confidentiality, 2) what is the procedure to be followed, 3) how national security is understood and 4) whether safeguards are necessary for the lifting of confidentiality of certain categories of persons. Although strict conditions for lifting confidentiality are set by the Constitution, specifying to a large extent the procedural scheme for lifting confidentiality, the four above themes are placed at the heart of the interest.<sup>32</sup>

### **3.1.1 Who is to authorise the lifting of confidentiality**

The lifting of confidentiality is within the powers of the judicial authority, as expressly laid down in the Constitution. Therefore, it is a constitutional choice to assign this responsibility to the judiciary, as a counterbalance to possible unfair use of lifting of confidentiality by the competent authorities. Thus, on the basis established by the 1994 implementing law and kept in the current legislation (Article 4 (2) of Law 5002/2022), the competent authority requesting the lifting of confidentiality for national security purposes submits a request to a public prosecutor who is called upon to decide within twenty-four (24) hours whether or not to proceed with the lifting. It is now provided that if there is an authorisation decision by the public prosecutor, then this, together with the file containing the request, is submitted to a second public prosecutor who is called upon within the same short period of time to approve or reject the request and return the file to the sender.

To begin with, there are two observations to be made on the above scheme. First, the possible lifting of confidentiality is approved by prosecutors, which from the outset implies guarantees of sound judgement and acts as a first filter for compliance with the Constitution. Second, judicial officers are obliged to approve or reject the lifting of the confidentiality by an extremely short deadline. The twenty-four (24) hour response deadline has been the subject of sharp criticism, since it severely limits the time judicial officers have to consider whether there is indeed a public safety purpose.<sup>33</sup> It has rightly been pointed out, on the other hand, that in matters of public security, time is of critical

---

Security and Privacy" and in Law 3649/2008 (Official Government Gazette A 39/03.03.2008) and in Law "National Intelligence Service (EYP) and other provisions " as amended by Law 4704/2020 and in force.

<sup>32</sup> Greek National Commission for Human Rights, 'Note to the Greek Parliament on the Bill of the Ministry of Justice and the Minister of State': "Procedure for the lifting of the confidentiality of communications, cybersecurity and protection of personal data of citizens" (December 2022) [https://www.nchr.gr/images/pdf/apofaseis/protaseis\\_epi\\_nomoth\\_keimenwn/Simeioma\\_EEDA\\_Aporito\\_epikoinonion.pdf](https://www.nchr.gr/images/pdf/apofaseis/protaseis_epi_nomoth_keimenwn/Simeioma_EEDA_Aporito_epikoinonion.pdf) last accessed 3 February 2023.

<sup>33</sup> Georgios Katrougalos, 'Freedom and Safety in the "Society of risk": Taking for instance, cases of monitoring' (2006) 54 3 Nomiko Vima 360-374,

importance<sup>34</sup> and that the tight time limit also places a kind of constraint on the authority requesting the lifting to assess the requests brought before the judicial officer.

Furthermore, pursuant to Article 5 (3) of Law 3649/2008 (as amended by Article 9 (1) of Law 5002/2022) concerning the National Intelligence Service (EYP), a public prosecutor shall be seconded to it, following a decision of the Supreme Judicial Council, for a three-year non-renewable term of office, in order to ensure the lawfulness of its specialised operational activities with regard to human rights issues. This specific provision has raised a lot of concern, despite the fact that its ratio is none other than to facilitate the functioning of the EYP and its operational activities. In other words, the secondment of a judicial officer responsible for this task helps to comply with the short time-frame of the lifting decision, allows for a quicker understanding of the requests and introduces a kind of informal supervision of the protection of rights during the operational activities of the EYP, by the judicial authority.

However, at times when there is information about possible unfair lifting of confidentiality based on pervading and non-individualised surveillance,<sup>35</sup> the question arises whether this provision has a positive effect or is likely to create a closed, non-controlled decision-making centre.<sup>36</sup> On the above-mentioned working case, it has been held that Article 5 (3) of Law 3649/2008 (as amended by Article 9 (1) of Law 5002/2022) undermines the guarantees scheme for lifting confidentiality and instead of the public prosecutor it would be preferable for a judicial council to decide, as it does in cases of particularly serious crimes. In fact, it was proposed that the decision should be taken by a judicial council on duty,<sup>37</sup> in order to achieve the time saving required by the legislator. At regulatory level, the provision does not weaken the guarantees scheme for lifting confidentiality, but instead establishes a more direct system of checks and balances between the judiciary and the executive powers.<sup>38</sup> In this context, the review of the request by a second prosecutor provides for an additional level of control, since the decision does not rest with a single person. Therefore, even in the event that the

---

<sup>34</sup> Georgios C. Sotirelis, 'Institutional and legislative challenges posed by the interceptions' (2022) 94 4 DtA 883-886.

<sup>35</sup> *Big Brother Watch et al. v. the United Kingdom*, App. nos 58170/13, 62322/14, 24960/15 (ECtHR, 25 May 2021) §495.

<sup>36</sup> Katerina N. Sakellaropoulou et al., *Justice in Greece, Proposals for a modern judicial system* (Athens: Dianeosis, 2019) 128-129.

<sup>37</sup> Maria Kaiafa-Gbanti, *Surveillance Models in the Security State & Fair Criminal Trial* (Athens: Nomiki Bibliothiki 2010) 45.

<sup>38</sup> Eyal Benvenisti & George W. Downs, 'Toward Global Checks and Balances' (2009) 3-4 ConstPolEcon 366-387, 385.

sound judgement of one prosecutor is questioned, the second check is carried out to remedy it.<sup>39</sup>

### 3.1.2 The waiver of confidentiality procedure

The common legislator also provides for the *minima* to be included in the order of the Public Prosecutor's Office (Article 4 (4) of Law 5002/2022), which are a) the body requesting the lifting, b) to what purpose the lifting serves, c) the means of response or communication to which the lifting applies, d) the subject matter of the lifting (external elements/metadata or content thereof), e) the territorial scope and duration of application, f) the date of issue of the order. The minimum prerequisites set out in the order of the Public Prosecutor's Office guarantee the legality of the lifting and define its scope.<sup>40</sup>

At this point, there are two interpretive and factual problems that arise. First, the prevailing practice has been for the provision not to give specific and in-depth reasons for the purpose of the lifting for national security purposes. While this is a provision with a content that is unfavourable to the subject of the right, there is no specific and fully-founded justification, since national security purposes also require appropriate secrecy.

Thus, the justification on which the provision is based is inherently insufficient in comparison with other acts restricting rights.<sup>41</sup> Secondly, it is extremely difficult to distinguish the limits set on the duration of the lifting of confidentiality. While a period of two (2) months is provided as the maximum time limit that may be ordered for the lifting of confidentiality, it is possible to extend it up to a maximum of ten (10) months,

---

<sup>39</sup> Aikaterina Papanikolaou, 'Withdrawal of confidentiality of Communications and the Obligation to communicate Information'. Lifting of Communication Confidentiality and Disclosure Requirements. A Question of Rule of Law Pending' (2022) 2 State Administration Inspectorate, 117-135, 124.

<sup>40</sup> The minimum standards provided for the lifting of confidentiality are also in line with the European acquis, where it sets out as prerequisites : a) a definition of the categories of persons whose confidentiality of their communications may have been lifted, (b) a time limit on the duration of surveillance, (c) the process to be followed for the examination, use and storage of the data collected, (d) specific arrangements for the transfer of data to third parties, (e) the circumstances in which intercepted data may or should be destroyed. *Huvig v. France*, App. no 11105/84, (ECtHR 24 April 1990); *Kruslin v. France*, App. no 11801/85 (ECtHR 24 April 1990); *Valenzuela Contreras v. Spain*, App. no 27671/95 (ECtHR 30 July 1998); *Weber and Saravia v. Germany*, App. no 54934/00, (ECtHR 29 June 2006).

<sup>41</sup> It is argued that the order of the Public Prosecutor's Office to lift the confidentiality is a pre-investigation procedure, a position that can be upheld in relation to the detection of particularly serious crimes. However, as regards the lifting of confidentiality on grounds of public security, what is at issue is an administrative measure which, for the purpose of ensuring more stringent safeguards, has been entrusted to a judicial authority. Konstantinos Giannakopoulos, 'Seeking more effective safeguards to ensure the confidentiality of communications' (2022) Constitutionalism <<https://www.constitutionalism.gr/anazitontas-apotelesmatikoteres-egiiseis-diasfalis-tou-aporritou-ton-epikoinonion/>> last accessed 3 February 2023.

while if there are national security purposes then the waiver of confidentiality may be in force for a longer period of time.

The time duration is by definition a key issue for the lifting of confidentiality. The lifting, as an exception to the confidentiality rule, must be limited in time and the legislation in force must provide for this.<sup>42</sup> In any other case, the very essence of the right to confidentiality of communications is affected, as the holder is deprived of the possibility to maintain the secrecy of his private communications. The common legislator sets a very high threshold for breaching the ten-month limit, as there must be a "direct and highly probable threat to national security" (Article 8 (4) of Law 5002/2022). The legislative basis for the justification and the particularly high threshold set for the prolonged surveillance period, raises a major question of balancing national security and protection of confidentiality. On the one hand, there is a reasonable question on the purpose of the lifting. That is, if there are such strong indications of a threat to national security that they do not cease, to what extent is the surveillance effective and no further action by the executive power is suggested. Of course, on the other hand, it is reasonable to observe that a threat to national security is at the core of any well-governed state, and if it occurs, it is the executive's obligation to safeguard it. Within this debate, of major importance is the justification for the waiver, which, although largely covered by the principle of secrecy, must clearly state the reasons for taking such an exceptional measure. The data in the file before the public prosecutor must fully substantiate that need. [Thus, the issue is again examined on the basis of the factual background of each case, subjected to the review of the proportionality of the measure in a strict sense.<sup>43</sup>

### **3.1.3 Defining the concept of "national security"**

The concept of national security is the biggest interpretative challenge to the lifting of confidentiality, since it is the assessment measure for both the requesting and the ordering authority. It is a vague legal concept, with a long interpretative history in all legal orders, as it is directly related to the rule of law. According to the settled theoretical and case-law approach, it is agreed that the choice of the term by the constitutional legislator against that of "public safety" was not a random one. Thus, the term "national security" has a very specific scope of definition and relates "exclusively

---

<sup>42</sup> *Iordache v. Romania*, App. no 6817/02 (ECtHR 14 October 2008).

<sup>43</sup> See, for example, Judgement of the Supreme Court Plenary Session 1/2017: Hellenic Council of State 1361/2013.

to what refers to the defence of the country against external threats<sup>44</sup> as opposed to public safety, which is clearly a broader term.<sup>45</sup>

In any case, however, it remains a vague legal concept that acts as a broad umbrella clause, to which the competent authorities of the judicial and executive powers, are called upon to assign those factual elements that put it at risk. In this context, one of the main legislative provisions introduced by Law 5002/2022 is the definition of national security grounds for the first time, as it was not included in the previous legislation. In Article 3 (a) it is stipulated that "national security purposes" are those related to the protection of the basic functions of the state and the fundamental interests of Greek citizens, such as, in particular, grounds related to national defence, foreign policy, energy security and cybersecurity.

First of all, there is a clear shift in the way the common legislator conceives the national security purposes justifying the lifting of confidentiality, as the above term broadens its conceptual content and includes new forms of risks. Besides the undeniable broadening, there is a tendency to modernise the term, as energy security and cyber security are added to the scope of the definition of national security. However, criticism is expressed regarding (a) the indicative list of reasons that constitute a risk to national security and (b) the reference to the basic functions of the state and the fundamental interests of the Greeks. With regard to the first part, the common legislator gives flexibility to the competent authorities to assess on what basis the national security is threatened. Whereas in the past only external threats against the State were understood as such, this exhaustive list no longer exists. As regards the second part, the reference to the basic functions of the state and the fundamental interests of Greeks comes closer to the concept of public security. This terminological broadening is a *prima facie* tendency to multiply the exceptions to the lifting of confidentiality.<sup>46</sup> But it is also indicative of the legislator's shift towards the internal legal order. Thus, national security is not exclusively an external risk, but on the contrary, it can also be found within the state. This provision is in line with the more specific regulation on the lifting of

---

<sup>44</sup> Chrysogonos(2006) 261.

<sup>45</sup> See in detail Giannis A.Tassopoulos, 'The Hollow Core of the Right to Confidentiality of Communications and National Security' (2022) 94 4 Dta Politeia 893-, 920.

<sup>46</sup>Between the definition settled by case law and the definition introduced by Law 5002/2022, the definition accepted by the ECtHR and following the standards of the United Kingdom is also proposed. In this respect, it is provided that 'national security is affected by *activities which threaten the security or welfare of the State and that are aimed at undermining or subverting parliamentary democracy* by political, industrial or violent means.'" See in detail Elissavet Symeonidou-Kastanidou, "The Bill on the Lifting of the Confidentiality of Communications: Critical to Fundamental Freedoms 'Failures' " (2022) constitutionalism <<https://www.constitutionalism.gr/to-sxedio-nomou-sxetika-me-tin-arsi-tou-aporitou-ton-epikoinonion/>> last accessed 3 February 2023.

communications confidentiality of political figures. In addition, the common legislator acknowledges that threats to national security may also arise from within.

At this point, the question arises as to the degree of fairness in adapting the regulatory framework to the actual situation. The above question is, of course, largely theoretical, since the success of the provision will be determined by its interpretation and application by the competent bodies. Following this assumption, the critical importance of the change in the term "national security" is more about the effective exercise of the powers of the National Intelligence Service (EYP) and the Special Violent Crime Squad (DAEEB or better known as Anti-Terrorist Unit) towards the public prosecution services. Here it is remarkable that the balance sought through the explicit provision that the lifting process on national security grounds is only hastened by the EYP and the DAEEB. Management of information collection by releasing confidentiality only to these two authorities confirms that the spirit of the law is to facilitate their functioning and effectiveness, rather than to diminish the safeguards of communications confidentiality. Certainly, this shifts the burden of proper implementation of the law to these two agencies, while increasing the need for more comprehensive institutional control over them.

### **3.1.4 Lifting of communications confidentiality of political figures**

Law 5002/2022 introduces for the first time increased guarantees for the activation of the mechanism of lifting the communications confidentiality of politicians, exhaustively listing who are understood as such (Article 3(b)). The additional guarantees set out in the legislation on the release of confidentiality of politicians are three: a) only the National Intelligence Service (EYP) shall submit a lifting request, b) before the request is sent to the prosecutor in charge, permission is granted by the President of Parliament within a short 24-hour period, c) there is a direct and extremely probable national security risk (Article 4 (3)(d) there is an immediate and extremely probable national security risk.

The relevant regulation has been put under the microscope, as it was largely imposed by political reality. The main points of the public debate are: (a) whether there is indeed a need for a specific provision for political figures and (b) whether the legislative provision is in accordance with the Constitution. The need for a specific provision for political persons is strongly contested,<sup>47</sup> primarily on the grounds that their position as

---

<sup>47</sup> The comparative review within the framework of the Council of Europe confirms the different approaches among the national legal orders of the Member States. In particular, it is stated that "[t]he immunity from prosecution varies from country to country and provides either full protection against detention and initiation of criminal proceedings without the permission of parliament (18 states) or partial protection, which does not cover members of parliament against interception or lifting of confidentiality of communications, police investigations and/or interrogation in case of arrest and/or against civil lawsuits, etc. (14 states). There is no provision for immunity from prosecution in the

bearers of the right to confidentiality of communications is not differentiated. Although the distinction between public and private life is not always clear, since they are public figures, the protection of the confidentiality of their communications lies outside this problematic.<sup>48</sup> However, the relevant regulation prevents the unfair use of lifting of confidentiality of political figures and at the same time reflects the criticality of their surveillance. The necessity of the regulation is based on the interaction of politicians with the political system and the critical nature of the information they may have in their capacity as major participants in public life. Therefore, the legislator tightens up the framework for the lifting of confidentiality in three ways. Apart from the high threshold of "direct and extremely probable risk" to national security that must be met, along with the possibility of a request for lifting only by the EYP, prior authorisation by the President of Parliament is the main measure to control and protect confidentiality.

The control by the President of Parliament is within the constitutional framework as it is in line with the provisions on the immunity from prosecution of certain persons (see Articles 62, 86 and 49 of the Constitution). Since the lifting of confidentiality places restrictions on the immunity of certain persons as provided for in the Constitution, prior authorisation by the President of Parliament is legitimate.<sup>49</sup> The common legislator follows the model of other countries, including France and Italy.<sup>50</sup> The authorisation by the President puts the executive's request for the lifting of the confidentiality of a political figure under the joint control of the legislature and the judiciary powers. The need to reach agreement on such a major issue is thus established, as the political

---

Netherlands." "There is no provision for the immunity from prosecution in the Netherlands." PACE, 'Parliamentary Immunity: Challenges to the Scope of the Privileges and Immunities Enjoyed by Members of the Parliamentary Assembly' (6 June 2016) Doc. 14076, <<https://pace.coe.int/pdf/2f15b3bbdea610373740e20cd47d54133cecfad2d831f9558b7404934552016e2/doc.%2014076.pdf>> last accessed 3 February 2023, 9-10, paragraph 19.

<sup>48</sup> Christina Akrivopoulou, 'The Privacy of Political Figures between the Public-Private Boundaries' (2009) 44 Dta 1283-1309, 1286-1287.

<sup>49</sup> Charalampos Anthopoulos, 'The Confidentiality of Communications of Political Figures' constitutionalism (2022) <<https://www.constitutionalism.gr/to-aporito-epikoinonias-ton-politikon-prosopon/>> last accessed 3 February 2023.

<sup>50</sup> Article 68 of the Italian Constitution provides that "...No member of Parliament shall be subjected to personal or home search, nor may they be arrested or otherwise deprived of their personal freedom, nor held in detention, without the authorization of their respective Chamber, save in the enforcement of a final court sentence, or when the Member is apprehended in the act of committing an offence for which calls for arrest *flagrante delicto*. The same authorization shall be required for Members of Parliament to be subjected to any form of interception of their conversations or communication and in order to seize their correspondence." The Italian Constitution expressly provides for the immunity of MPs to include the confidentiality of their communications and that in the event of this being lifted, prior authorisation must be obtained from Parliament.

dimension of the lifting of the communications confidentiality of a political person is by definition great.

Finally, special mention should be made of the fact that the President of the Republic is included in the list of political figures who may be subject to the lifting of the confidentiality of communications. The possible lifting of confidentiality of the person of the state institution who is the guardian of the constitution raises particular issues, since the foundations of the constitutional organisation are also called into question. In a case where there is a direct and highly probable threat to national security that justifies the lifting of confidentiality of the President of the Republic, then we are obviously outside the framework of constitutional normality.

#### **4. The establishment of an independent authority for the protection of communications**

Article 19 (2) of the Constitution provides for the establishment and operation of an independent authority to safeguard the confidentiality of communications. The above constitutional provision was added to the list of guarantees for the protection of the right with the revision of 2001, while implementing Law 3115/2003 established the Hellenic Authority for Communication Security and Privacy (ADAE).<sup>51</sup> ADAE replaced the National Committee for the Protection of Communications Privacy (EthEPAE) provided for by implementing Law of Article 19 of the Constitution (Law 2225/1994) and enhanced oversight against unfair use of the lifting of communications confidentiality by the executive.<sup>52</sup>

The establishment of the ADAE was a necessity, since both the national situation and the international challenges, together with technological development, in a way imposed that it be created.<sup>53</sup> Now, the proceedings before the ADAE and its operation have helped to clarify critical issues related to the confidentiality of communications.<sup>54</sup>

#### **4.1 Constitutional provisions for the independent authorities (Article 101A of the Constitution)**

The 2001 revision of the Constitution played a key role in the creation and development of the independent authorities. Apart from specific provisions for the establishment of five (5) independent authorities, in Article 101A of the Constitution was introduced the

---

<sup>51</sup>Law 3115/2003 (Official Government Gazette A'47/27.2.2003) "Hellenic Authority for Communication Security and Privacy".

<sup>52</sup> Papadopoulos (2017) 486.

<sup>53</sup> Charles Tiefer, "The Constitutionality of Independent Officers as Checks on Abuses of Executive Power" (1983) 63 1 BULRev 59-103, 70-76.

<sup>54</sup> See for example Council of the Hellenic Council of State 359/2020, 3319/2010, 3320/2010, Hellenic Council of State 3473/2017.

basic framework for their operation.<sup>55</sup> The legal and political system welcomed the constitutional foundation of independent authorities. As it is rightly pointed out, “independent authorities are [...] a form of strengthening and protecting the rule of law ideal, but at the same time a manifestation of the deep crisis of the democratic ideal”. A view which suggests that their establishment also expresses, *inter alia*, the attempt to neutralise very serious areas of state power.<sup>56</sup> (See also Article 2 (b) TFEU.)

According to the prevailing interpretation of Article 101A of the Constitution, independent authorities are not *aliud*, but a part of the administration.<sup>57</sup> Although they deviate from the model of its pyramidal organisation, because they are not subject to any kind of administrative supervision, they remain part of the administration.<sup>58</sup> The main constitutional characteristics attributed to them relate to the way they operate and are organised. The main institutional characteristics are the fixed term of office of the members (a) and their individual and functional independence (b).<sup>59</sup>

In fact, it is acknowledged that their two constitutionally provided elements operate in a balancing manner, since the fixed term of office sets a limit to the functional and individual independence of the members, namely when the powers of the independent authorities are expanded and assume regulatory, repressive and sanctioning actions.<sup>60</sup>

## 4.2 Legislative and institutional framework of operation of the Hellenic Authority for Communication Security and Privacy (ADAE)

The ADAE was first established as an institutional guarantee for the protection of the confidentiality of communications. However, in the course of its operation other functions have been included and it now exercises a peculiar control over the administration. With regard to the powers of the ADAE as originally provided for in Article 6 of Law 3115/2003, as amended and in force, the focus is on its powers of control. As it follows from the literal interpretation of the legal framework, the ADAE carries out controls either to ensure that the conditions for lifting the confidentiality

---

<sup>56</sup> Evangelos Venizelos, ‘Independent Authorities after the Revision of the Greek Constitution of 1975/1986/2001 (29 October 2002) <<https://www.evenizelos.gr/127-programm-proposals/state/transparency/1120-197519862001.html>> last accessed 3 February 2023.

<sup>57</sup> Evgenia Prevedurou, ‘What are the independent authorities and what are they for’ (12.05.2019) syntagmawatch <<https://www.syntagmawatch.gr/my-constitution/ti-ine-oi-anexartites-arches-kai-se-ti-chrisimevoun/>> last updated on 3 February 2023.

<sup>58</sup> Epameinondas P. Spiliotopoulos, *Handbook of Administrative Law*, p. 1 (13<sup>th</sup> ed., Athens: Nomiki Bibliothiki 2010) 293.

<sup>59</sup> Katerina Iliadou, ‘Article 101A’ in F. Spyropoulos et al., *The Constitution of Greece, Article by article interpretation* (Sakkoulas Publications: Athens – Thessaloniki, 2017) 1623-1633, 1627.

<sup>60</sup> Papadopoulos (2017) 1627.



procedure are respected, or to detect whether extra-institutional interceptions are taking place.<sup>61</sup>

The purpose of this legality check is, in the first case, to ensure procedural compliance with the terms and conditions laid down by the legislator for the lifting and in the second case to determine whether private communications are being intercepted. In both cases, the audit function of the ADAE focuses on the formal elements that must be met for the lifting of confidentiality. In other words, the audit function is limited to the formal elements of the legality of the lifting and does not interfere with the substantial part of the lifting (as long as it is a legal connection).<sup>62</sup>

The issues raised in relation to the power of control of the ADAE are mainly three. First, what is the role of the ADAE in the event that an extremely high number of cases of lifting of confidentiality is detected, or of cases of lifting of confidentiality as regards a number of persons of institutional importance for national security, but who meet the legal requirements. In other words, if the controls carried out reveal a pattern of multiple cases of lifting of confidentiality that is inconsistent with the usual data over the years, or the targeting of individuals with an institutional role in the State organisation, then the question is, *what is the appropriate action to be taken by the ADAE?* The question arises from the constitutional foundation of the independent authority as an additional institutional guarantee to ensure confidentiality. Given that it is impossible for the ADAE to get involved in the substantive part of the lifting requested by the competent authorities and approved by prosecutors, reporting, as required by law, is a crucial element. Therefore, there is a duty to inform on the basis of the data in any given situation, if it suggests that legitimate and formally adequate operations of lifting of confidentiality are either being carried out unfairly or indicate the existence of a serious risk to national security. It's about a delicate balance, where the ADAE, relying on formal, external elements obtained from an audit, makes a substantive assessment and provides information as required. At this point, it is rightly highlighted that the power

---

<sup>61</sup> Nikos Papaspyrou, 'The responsibilities of ADAE and the rule of law' (2022) constitutionalism <<https://www.constitutionalism.gr/oi-armodiotites-tis-adae-kai-to-kratos-dikaiou/>> last updated 3 February 2023.

<sup>62</sup> See for example: ADAE, '2021 Activity Report' <[http://www.adae.gr/fileadmin/press/EKTHESI\\_PEPFRAGMENON\\_ADAE\\_2021.pdf](http://www.adae.gr/fileadmin/press/EKTHESI_PEPFRAGMENON_ADAE_2021.pdf)> last updated 3 February 2023, 57-58. "In the context of the principle of the separation of powers, the ADAE certainly refrains from expressing positions which are intrinsic to the substance of the judicial judgement and which concern, in essence, the advisability of pursuing the special investigative measure in question. It is, however, obliged, in the context of examining the legality of orders for the lifting of confidentiality, to verify whether there is a justification as a procedure, or not, and to record cases concerning unjustified orders cases or cases based on formal reasons, such as, for example, the mere repetition of a legislative provision. Given that the law requires, in each case, a specific and detailed justification, it is clear that the Authority's comments on this are part of its obligation to ensure that the legal safeguards are respected."

of control of the ADAE lies at the core of its operation and if it is diminished, this will also diminish its work.<sup>63</sup> Similarly, it is also necessary to define the limits of this power, so that it does not intrude into or overlap with the work of the judiciary.

The second point of interest is directly related to the first and seeks to ensure safeguards for the protection of personal data when carrying out the relevant controls. This is an issue of concern to the ADAE since its establishment, as the constitutional foundation of independent authorities for the protection of personal data and protection of confidentiality may lead to an overlap of competences. After all, private communications of an intimate nature involve personal data from the outset.<sup>64</sup> The chances increase as technological progress reshapes the communications landscape. In addition, the competences of the ADAE co-exist along with the regulatory powers of other administrative entities, such as the Hellenic Telecommunication and Post Commission (EETT).

In this light, the need to unify the institutional framework and institutionalise cooperation among independent authorities is imperative. Moreover, the lifting of communications confidentiality requires by definition the processing of personal data, bearing in mind that the former includes both internal and external contact details. As a result, unified and integrated legislation, at the substantive, procedural and supervisory level, on the protection of data and communications will enhance both the protection of data subjects and the duty to inform the independent authorities. It would therefore be beneficial to institutionalise cooperation or even synergy among the stakeholders involved, especially the independent authorities, rather than relying entirely on good practices adopted by their members.<sup>65</sup>

The third point of contention is about notifying the data subject of the lifting of confidentiality of his/her communications and the subsequent processing of the material. The lifting of confidentiality of communications is in principle a violation of a constitutionally enshrined right, which is exceptionally permissible for national security purposes or when it is necessary to investigate a serious crime. However, the subject of the right remains the bearer of the right and therefore there is always the

---

<sup>63</sup> Charalampos Anthopoulos, 'Constitutional experts and the Dogiakos' Opinion' (2023) constitutionalism <<https://www.constitutionalism.gr/oi-sintagmatologoi-kai-i-gnomodotisi-ntogiakou/>> last accessed 3 February 2023.

<sup>64</sup> In detail, see also the relevant Opinion of the Prosecutor of the Supreme Court, Georgios Sanidas, No 9/2009 (Reference No 2726) 29 June 2009 <<https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-09-2009/>> last accessed 1 March 2023, 12.

<sup>65</sup> Hellenic Authority for Communication Security and Privacy, 'Meeting of the President of the Authority with the President of ADAE' (Press Release) (22.07.2019) <<https://www.dpa.gr/el/enimerwtiko/deltia/synantisi-toy-proedroy-tis-arhis-me-ton-proedro-tis-adae>> last accessed 3 February 2023.

possibility of judicial protection and control of the legality of the withdrawal. A crucial point is whether and when the subject can be notified of the lifting of the right. As regards the question of possibility, there is no uniformity in the legal framework.<sup>66</sup> However, it is unanimously considered that it is not possible to notify the subject at the time of the lifting of the confidentiality, as this would invalidate the effectiveness of this exceptional measure. Therefore, the lifting of confidentiality constitutes in principle a derogation from the provisions of the General Data Protection Regulation (GDPR),<sup>67</sup> as well as the Council of Europe Convention 108/1981 on the Protection of individuals with regard to automated processing of personal data.<sup>68</sup>

The new legislative framework has an explicit provision on the procedure and conditions for the notification of the lifting of confidentiality to the data subject and the subsequent management of the surveillance material (processing file). The relevant provisions have been criticized by both ADAE<sup>69</sup> and the Hellenic Data Protection Authority (DPA),<sup>70</sup> as they are considered to significantly restrict the right of a citizen who has had his or her communications legally lifted, to have access and be relatively notified of, or to challenge the legality of the lifting, with access to a fair trial. The lack of more specific provisions for the exercise of these rights makes it more difficult for those who have had their confidentiality lifted to be relatively notified of, unless it is necessary for national security purposes. Of course, the lack of specific provisions in Law 5000/2022 does not exclude the general provisions to be applicable, while the broader European *acquis* that the ECtHR has set with its case law is also taken into

---

<sup>66</sup> See also amendment 826/145/31-3-2021 on the amendment of Article 5(9) of Law 2225/1994 stipulating that '[a]fter the termination of the lifting measure and provided that the purpose for which it was ordered is not compromised, may the ADAE decide to notify its enforcement to the affected persons' and Article 87 of Law 4790/2021 which has completely abolished the possibility of notifying the citizen of the lifting of confidentiality of his communications, according to which "[a]fter the termination of the lifting measure and provided that the purpose for which it was ordered is not compromised, may the ADAE decide to notify its enforcement to the affected persons."

<sup>67</sup> Hellenic Data Protection Authority, 'Lifting of Confidentiality of Telecommunication Services and Lifting of Notification of the Data Subject' (Opinion 1697, 15.12.2000) <<https://www.dpa.gr/el/enimerwtiko/prakseisArxis/arsi-aporritoy-ton-tilepikoinoniakon-ypiresion-kai-arsi-enimerosis>> last accessed 3 February 2023.

<sup>68</sup> CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108, 28.1.1981) <<https://rm.coe.int/1680078b37>> last accessed 3 February 2023.

<sup>69</sup> ADAE, '2021 Activity Report' <[https://www.avgi.gr/sites/default/files/2022-11/Pepragmena\\_2021.pdf](https://www.avgi.gr/sites/default/files/2022-11/Pepragmena_2021.pdf)> τελευταία ενημέρωση 3 Φεβρουαρίου 2023, 69.

<sup>70</sup> Hellenic Data Protection Authority, Opinion on the Bill entitled, 'Procedure for the lifting of the confidentiality of communications, cybersecurity and protection of personal data of citizens' (Opinion No 5, 25.11.2022) <<https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gnomodotisi-epi-toy-shedioy-nomoy-diadikasia-arsi-toy-aporritoy-ton>> last accessed 3 February 2023.

consideration.<sup>71</sup> Thus, the fact that there is a right to notification at least three years after the termination of the lifting of confidentiality, while it is in parallel provided that the evidence is destroyed within six months, raises questions about how useful it is to notify the affected person.

In practice, the common legislator has struck a critical balance between the data subject's right to be relatively notified of and the national security and sets a strict framework for the further notification of the individual. In fact, the time limit that must elapse before it becomes possible for the private individual to be notified of, weakens his or her rights by definition and does not facilitate the administration of justice. The role of the ADAE in this respect is neither to oversee nor to audit, since the independent authority notifies the person affected. The question remains whether the notification procedure provided for ensures the right to judicial protection of the person affected and respect for private life as a whole.<sup>72</sup>

#### **4.3 Constitutional obligations to be fulfilled by independent authorities and the ADAE, as set out by the common legislator**

Indeed, the legislative provisions on the lifting of confidentiality clearly affect the operation of the ADAE to an extent that its institutional role is being modified in cases where confidentiality is lifted, especially for national security purposes. Three conclusions can easily be drawn from the above.

First, the legal and political landscape as it has evolved requires coordination and cooperation among the independent authorities whose competences overlap in the field of communications confidentiality. In this respect, the legislative provision for cooperation among the ADAE the DPA and the Hellenic Telecommunications and Post Commission (HTPC) is imperative, not only in order to deal more effectively with cases of lifting of confidentiality, but also with other priority issues, such as the use of malicious software for illegal surveillance. Cooperation among the independent authorities also implies a fruitful dialogue to streamline their powers and optimise their way of operation.

Consequently, the need to redefine the competences of the independent authorities arises at a second level. Despite the fact that their competences are being increasingly extended, there is an expectation that they will become more involved in matters of

---

<sup>71</sup> Of course, it is noted that the ECtHR allows for a wide discretion to the Member States, as the lifting of confidentiality is required for purposes that lie at the core of state sovereignty. Thus, the ECtHR underlines that lifting of confidentiality is tolerable "to the extent that it protects the democratic institutions of a State". Steven Greer, *The Margin of Appreciation: Interaction and disruption under the European Convention on Human Rights* (Strasbourg: CoE Publishing 2000) 36.

<sup>72</sup> CoE, Information Society Department, 'Pegasus Spyware and its Impacts on Human Rights' DGI (2022)04 <<https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8>> last accessed 3 February 2023.



rights protection. In particular with regard to the ADAE, its constitutional foundation as an institutional safeguard for the confidentiality of communications reasonably raises the expectation that it will also become involved in cases where it is lifted. However, given that independent authorities cannot substitute the judiciary, their powers of control are determined by their administrative nature, and hence they cannot control the unconstitutionality of laws. In those procedures where an opinion of judicial officers is required, the legislator introduces a strong procedural guarantee. Therefore, the procedure for lifting the confidentiality of communications in both cases sets a robust framework both in terms of safeguarding national security and the affected subject. In this context, the audit function of the ADAE is carried out in a specific way, aiming at being effective, without putting into question the safeguards relating to the lifting of guarantees. Thus, the submission of activity and special reports, as well as the hearing of the President of the ADAE and the right to report to Parliament, become increasingly important. These are the institutional means available to the independent authority to point out possible malfunctions in the lifting of confidentiality proceeding and to bring them under parliamentary oversight.

Third, the lifting of confidentiality and the technological development that determines communications raises a major issue of processing and storage of personal data during and after the lifting has been carried out. Thus, the protection of the privacy of the persons affected not only covers the lifting of confidentiality, but also ensures that the content of their communications will not be disclosed to third parties other than the bodies responsible for this purpose.

### **C. Confidentiality of communications in other legal orders**

The legislative and broader institutional framework for the lifting of communications confidentiality is a challenging task for several national legal orders as well, especially for those where technological developments have given priority to electronic communications.

There is a great diversity of the institutional framework in each national legal order,<sup>73</sup> as it is largely influenced by the constitutional system of each one. A key common element is the attempt to balance national security and public order with the right to confidentiality of communications. The comparative overview of legal orders demonstrates the main existing variations, in particular among the Member States of the European Union.

---

<sup>73</sup> UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin 'Ten areas of best practices in countering terrorism' (22 December 2010) UN Doc A/HRC/16/51, <<https://www.refworld.org/docid/4e0c2ace15.html>> last accessed 3 February 2023.

## 1. Comparative overview within the European Union

The investigation and comparative review of the wider institutional framework of EU Member States with regard to the collection of information and the prior lifting of confidentiality of communications became a necessity due to revelations about mass surveillance of individuals,<sup>74</sup> but also because the risk of terrorist attacks led several countries to tighten up their legislation.<sup>75</sup> Furthermore, there is now a shift in the interest of intelligence services to private individuals and not necessarily to state actors.<sup>76</sup>

At first sight, the areas that appear to be homogeneous between the EU Member States are: A) the way intelligence services are organised. The model of the establishment and operation of a specific agency responsible for intelligence collection to ensure national security is applied, with minor variations. Intelligence agencies are by definition under the executive power and subject to the highest level of control. Their heads are appointed and dismissed by the prime minister (as the head of the executive) in several countries, such as France, Poland and Italy. In fewer countries, intelligence services are under the Ministry of Citizen Protection, such as the Netherlands. It should be noted that in Greece, EYP was also under the Ministry of Citizen Protection, while in recent years it is under the direct supervision of the Prime Minister. B) There is limited knowledge and little research on the exact structure and operation of intelligence services in all countries, with vague provisions in the relevant legislation. Despite the fact that clarity of the primary legislation is one of its fundamental elements, the provisions concerning the precise internal operation of intelligence services appear to constitute a quasi-exception to the rule, which is deemed legitimate in order to protect national security and safeguard their effectiveness.<sup>77</sup> C) In all Member States a special law is required to provide for the intelligence collection and to allow for the confidentiality to be lifted in exceptional cases. The existence of legislation is a primary challenge to the existence of the rule of law. D) Furthermore, in the EU countries, the

---

<sup>74</sup> Dave Snowden & Alessandro Raccati, *Managing Complexity (and Chaos) in Times of Crisis: A Field Guide for Decision Makers Inspired by the Cynefin Framework* (Luxemburg: Publications Office of the European Union 2021).

<sup>75</sup> UN Working Group on Protecting Human Rights while Countering Terrorism, *Basic Human Rights Reference Guide, Security Infrastructure* (New York: CTITF Publication Series 2010).

<sup>76</sup> European Union Agency for Fundamental Rights (FRA), *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, Volume I: Member-States' Legal Frameworks* (Luxemburg: Publications Office of the European Union, 2017) 14.

<sup>77</sup> See in detail, Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Towards Harmonized Data Protection Principles for Information Exchange at EU-Level* (Berlin: 2012 2012) 58.



actions of intelligence services do not escape judicial scrutiny following the lifting of confidentiality and surveillance of individuals.<sup>78</sup>

The above constitute the indisputable points of convergence among the national legal orders of the European region. But there are clearly more variations and they concern three main areas: (a) the purposes for which a lifting can be ordered (b) the supervisory authorities of the intelligence services and (c) the means available to the person affected to challenge the lifting of his or her confidentiality and defend his or her rights.

### 1.1 Comparative review of the lifting of confidentiality purposes

The lifting of confidentiality and the interception of private communications and correspondence are provided for as an exception to the rule in national legal orders. However, the purposes justifying the lifting vary. First of all, in the majority of countries the lifting of confidentiality is targeted or strategic. In other words, one or more individuals are clearly defined or easily identifiable through their capacities. By contrast, in some countries, it is possible for the intelligence services to carry out generalised surveillance in the event of an exceptional risk to national security.<sup>79</sup> These are mainly countries that have suffered terrorist attacks and have tightened up their national security protocols, at the same time facilitating the surveillance of large numbers of subjects. The United Kingdom is one of them.<sup>80</sup>

In addition, the lifting of confidentiality should be specifically and reasonably provided for by law. This criterion is directly related to the quality of the legislative framework and any comparative assessment is even more difficult. However, it is worth noting that there are national legal orders that allow for the lifting of confidentiality on the basis of reasonable suspicion (suspicion based surveillance), which may be based on behaviours, categories of persons, local, personalised or of a protective nature parameters.<sup>81</sup> Most of the time, such cases of lifting of confidentiality are partially randomized, thus reducing the guarantees of protection of individuals.

---

<sup>78</sup> Damian Chalmers, Gareth Davies & Giorgio Monti, *European Union Law* (4<sup>th</sup> edn, Cambridge: CUP 2019) 445.

<sup>79</sup> Christopher Prince, 'On Denoting and Concealing in Surveillance Law' in David Lyon & David Murakami Wood (eds) *Big Data Surveillance and Security Intelligence, The Canadian Case* (Toronto: UBC Press 2021) 43-56, 49.

<sup>80</sup> Eliza Watt, 'The right to privacy and the future of mass surveillance' (2017) 21(7) *The International Journal of Human Rights* 773-799.

<sup>81</sup> Pieter Wagenaar & Kees Boersma, 'Zooming in on 'Heterotopia': CCTV-Operator practices at Schiphol Airport' in C. William R. Webster *et al.* (eds) *Video Surveillance, practices and policies in Europe* (Amsterdam: IOS Press 2012) 66-79, 69.

## 1.2 Intelligence services oversight bodies

There are more legislative differentiations with regard to the oversight bodies of intelligence agencies. A particular diversity can be observed, as there is parallel a control over the intelligence services by the executive (to which they are directly subject), but also by parliamentary bodies, the judiciary or independent authorities.

Apart from their administrative subordination to the executive and the exercise of parliamentary control over their budgets, there is little in common among EU member states. The possible unfairly used interpretation and application of the legislative framework by intelligence services is, in some Member States, controlled by special parliamentary committees<sup>82</sup> or in other cases by independent authorities. There are therefore two trends observed with regard to the control over intelligence services (parliamentary vs expert oversight). Thus, according to the existing data, in thirteen (13) out of the twenty-seven (27) EU Member States, the control over intelligence services falls under the limits of ordinary parliamentary control (e.g. defence committees).<sup>83</sup>

As regards the independent authorities tasked with auditing possible breaches in the lifting of confidentiality, differentiations can also be observed. For example, in Germany and Poland, the work of the Greek ADAE has been taken over by the national anti-corruption authorities. In these legal orders, the misapplication of law and the exercise of powers is subject to the broader field of corruption and is not related to the right to confidentiality of communications. In other words, it is a matter of administrative malfunction and not an institutional guarantee of a right. In the same vein the French example, where the control of the operation over the French intelligence service is exercised by the "National Commission for the Control of Technical Information"(Nationale de Contrôle des Techniques de Renseignement, CNCTR). In the French legal order, the risk at stake is not rooted in the right of the individual affected, but in the uncritical collection of intelligence. For this reason, oversight bodies focus on the way intelligence is collected.<sup>84</sup> Finally, there is the particular case of the United Kingdom where oversight and control are exercised by a unit of the national

---

<sup>82</sup> Marina Caparini, 'Controlling and Overseeing Intelligence Services in Democratic States' in Hans Born & Marina Caparini (eds) *Democratic Control of Intelligence Services* (London: Ashgate 2016) 3-24.

<sup>83</sup> European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, 'The Use of Pegasus and Equivalent Surveillance Spyware, The Existing Legal Framework in EU Member States for the Acquisition and Use of Pegasus and Equivalent Surveillance Spyware' (December 2022) PE740.151, 82.

<sup>84</sup> Bertrand Warusfel, 'The Intensification of French Intelligence and its Oversight under the Impact of Counter-Terrorism' in Ian Leigh & Njord Wegge (eds) *Intelligence Oversight in the Twenty-First Century* (London: Routledge 2018) 124-134.

intelligence service, which operates in line with the internal quality assurance principles (legality within the agency). The audit function is performed through random audits.<sup>85</sup>

Finally, particular reference should be made to the relation between the intelligence services and the data protection authorities. In the European Union, the protection of personal data encompasses the basic freedoms of the subject and there is a strong emphasis on their protection. Thus, especially after the entry into force of the GDPR, the obligation of European countries to ensure the protection of personal data has a supranational basis. On this point there is a complete lack of coherence among national legal orders. In some cases, national data protection authorities have full power of over the intelligence services, in others they have reduced powers, while in others there is no administrative contact and no operational interconnection.<sup>86</sup>

### **1.3 Oversight delimitation and exercise of powers of control over intelligence services**

Intelligence services are supervised by various bodies such as the judiciary power, independent authorities, parliamentary committees and expert bodies. Oversight is crucial as it helps to ensure the accountability of intelligence services and to develop effective internal guarantees. Intelligence oversight and the structure of the agencies involved pose a challenging task within most national legal orders. The problematic issues that national legislators are called upon to address are summarised in nine (9) topics: a) why it is important to oversee the intelligence services and why it is important to clearly delineate the responsibilities of the various agencies involved b) how to ensure the effectiveness of the oversight mechanisms, whether in the case of parliamentary or independent control c) whether it is possible to achieve transparency in the way the intelligence services operate, without compromising the principle of secrecy that governs them and how this is compatible with a democratic constitution d) what is the appropriate way to exercise control and submit relevant reports, (e) if and when intelligence can be collected and by which agency (f) how the protection of personal data is safeguarded (g) what kind of intelligence can be disclosed (h) how the financial audit of the intelligence services is carried out and (i) who is the competent body to handle complaints about interception and lifting of confidentiality by the intelligence services.<sup>87</sup>

---

<sup>85</sup> Lorna Woods, 'The Investigatory Powers Act 2016' (2017) 12 *Journal of Data Protection & Privacy* 222-232, 228. See in particular about the Investigatory Powers Commissioner's Office <<https://www.ipco.org.uk/ocda/>> last updated on 3 February 2023..

<sup>86</sup> FRA (2017) 49.

<sup>87</sup> Hans Born & Gabriel Geisler Mesevage, 'Introducing Intelligence Oversight' in Hans Born & Aidan Wills (eds) *Overseeing Intelligence Service, A Toolkit* (Geneva: DCAF, 2012) 3-24, 12.

As mentioned above, the ex-post oversight on the proper functioning of intelligence services, as regards the unfair or non-use of cases of confidentiality lifting, is entrusted either to specialised non-parliamentary supervisory bodies (which in the Greek legal order take the form of an independent authority), or to the Parliament, where special committees are set up for this purpose.

In both cases there are pros and cons. In the case of special authorities set up by experts (such as the ADAE), the experience of their members and the fact that they are charged exclusively with this task is a key element, unlike parliamentary committees, which undertake this role within the framework of their broader competences. Furthermore, independent authorities or equivalent bodies are composed of persons not engaged in political activity and therefore the weight of their choices is not politically relevant.<sup>88</sup>

Ex-post general oversight on cases of lifting of confidentiality falls within the powers of control of independent authorities or parliamentary committees. By contrast, individualised control is usually a matter for the courts. Despite the fact that the administrative structure in all legal orders is based on the clearly delimited competences of the institutions, in the specific case with regard to the oversight on intelligence services, it seems more appropriate and democratically safer that the oversight bodies' mandates should be complementary. This is one of the exceptional cases where overlapping is considered to be positive, as the existence of a single oversight mechanism is potentially dangerous and inadequate.<sup>89</sup> For example, the intelligence surveillance system in Italy has recently been updated. After the lifting of confidentiality, in addition to the individualised oversight that can be carried out by the competent judicial bodies on the initiative of the affected person, it is possible that the oversight will be conducted by the Office of the Inspector General (which is a one-person internal administrative body) and by the Parliamentary Committee on the Security of the Republic (COPASIR).<sup>90</sup>

The ex-post oversight on the legality of lifting of confidentiality for public safety purposes should be distinguished between general and individualised. In cases where the legality control is initiated by the affected person, it should be exercised by the competent courts. However, other legal orders provide that independent authorities or

---

<sup>88</sup> Iain Cameron, 'Oversight of Intelligence Agencies: The European Dimension' in Zachary K. Goldman et al. (eds) *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford: OUP 2016) 71-94, 78.

<sup>89</sup> CoE, Venice Commission, 'Report on the Democratic Oversight of Signals Intelligence Agencies' (20-21 March 2015) CDL-AD (2015)011 8-9.

<sup>90</sup> Stefania Ducci, 'The Italian Parliamentary Intelligence Oversight Committee, An Analysis in the Light of International Legal Standards and Best Practices' (December 2009) Rieas Research Paper No. 138, 7.



specialised courts may deal with individual complaints.<sup>91</sup> With regard to the general oversight on the legality of the lifting of confidentiality by the intelligence services, it is noted that the ways it is carried out and the delimitation thereof, vary according to the State organisation and the constitutional culture of each State.<sup>92</sup>

Parliamentary oversight is provided for in all countries, while in some of them this control is exercised in parallel with an independent authority or a special body. The oversight of independent authorities (or, in general, committees of experts) is finalised in the form of reports, the final recipient of which is the parliament or the highest collective body of the State. In this case, the relevant parliamentary committee is called upon to assess the results presented, while retaining full autonomy in the exercise of its powers of control. France is one such case.<sup>93</sup> In other words, parliamentary oversight on the legality of lifting of confidentiality by the intelligence services is not undermined by the fact that oversight is carried out by independent bodies as well. After all, this is why, in several countries, parliamentary oversight is the only one that exists. Parliamentary oversight is therefore exercised in the first instance, but can also be exercised *ex post* on the reports submitted by the specialised administrative bodies.

Obviously, the quality of oversight between parliamentary committees and independent authorities is by definition different. Bodies of experts, similarly with independent authorities, are primarily concerned with ensuring the legality of the oversight and that rights are not abused or systematically violated. On the other hand, parliamentary oversight is clearly reflecting political implications and connotations, and thus there is greater flexibility when it comes to assessing public security risks.<sup>94</sup>

From the above, it becomes apparent that while comparisons among national legal orders are not clearly discernible, there are some constitutional standards. First, in democratic regimes where the principle of parliamentarianism is at the core of the State organisation, parliamentary oversight remains unaffected and independent of the

---

<sup>91</sup> Thorsten Wetzling & Kilian Veith, *Upping the Ante on Bulk Surveillance, An International Compendium of Good Legal Safeguards and Oversight Innovations* (Berlin: Heinrich Böll Foundation) 12.

<sup>92</sup> The control of information services in most countries is only a legality check (e.g. Sweden and Denmark), while in fewer cases the control exercised is more extensive and covers the efficiency, effectiveness and legality of their actions. Such an example is the United States.

<sup>93</sup> Felix Treguer, 'Major oversight gaps in the French intelligence legal framework' (2022) <<https://aboutintel.eu/major-oversight-gaps-in-the-french-intelligence-legal-framework/#:~:text=In%202021%2C%20the%20French%20government,international%20standards%20in%20intelligence%20oversight.>> last updated 3 February 2023.

<sup>94</sup> Samuel Stolton, 'Council of Europe calls for greater oversight on intelligence community's surveillance powers' (2020) <<https://www.euractiv.com/section/digital/news/council-of-europe-calls-for-greater-oversight-on-intelligence-communitys-surveillance-powers/>> last updated 3 February 2023.



existence of any specialised administrative bodies (see, for example, the case of Germany and the United Kingdom).<sup>95</sup>

Therefore, the two types of control may be exercised in parallel with overlapping functions in place, with full autonomy of the bodies exercising it, remaining unaffected. Whereas parliamentary oversight derives directly from the will of the people, in the case of independent authorities their powers of control derive from the Constitution or they are established to protect constitutionally enshrined rights.

The one requirement that seems to be gradually emerging in the form of 'good practice' is cooperation among the committees and bodies exercising control over the intelligence services.<sup>96</sup>

#### 1.4 Effective legal remedies for persons affected

The last area covered by the comparative review refers to the remedies available to the persons affected following the lifting of their confidential communications. The basic assumption running through all national legal orders is that the subjects must be able to be notified of the lifting of their confidential communications and have access to the records held by the intelligence services concerning them. These are also the necessary conditions for them to have access to a fair trial should they challenge the legality of their surveillance. Nevertheless, there is a general difficulty for individuals to exercise these rights, which makes the effectiveness of the means provided doubtful or even weak.

First, access to national courts is difficult because of the restrictions imposed by the common legislator on individuals' rights to be notified and access the courts (the elimination of the national security purposes, the termination of a period of time, etc.). Furthermore, as regards the means available to the subjects to raise objections, the information provided is also insufficient.<sup>97</sup> Overall, a low level of protection of this right is observed in most legal orders. Even in those Member States where access to ombudsmen is provided for or specific remedies are available, the necessary protection is yet to be achieved.<sup>98</sup>

---

<sup>95</sup> Andrew Defty, 'Familiar but not intimate': Executive oversight of the UK intelligence and security agencies' (2022) 37(1) *Intelligence and National Security* 57-72, 60.

<sup>96</sup> Hans Born & Ian Leigh, 'Democratic Accountability of Intelligence Services' in Hans Born & Ian Leigh (eds) *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (Oslo: Publishing House of the Norwegian Parliament, 2005) 193-214.

<sup>97</sup> Hungarian Helsinki Committee (HHC) & European Council on Refugees and Exiles (ECRE), 'Effective Remedies in National Security –Related Asylum Cases, with a Particular Focus on Access to Classified Information' (2022) Legal Note #12 <<https://ecre.org/wp-content/uploads/2022/05/Legal-Note-12.pdf>> last accessed 3 February 2023

<sup>98</sup> FRA (2017) 75- 76.

## D. Concluding Observations

The redesign of the Greek regulatory framework should be pursued along two axes. Firstly, on the basis of a **fair balance between confidentiality and national security** and secondly, on taking into account **technological advances**. A comparative review of the legislative arrangements in other European countries shows that the Greek legal order interprets the issue of the control over security services and the lifting of communications confidentiality, from the strict point of view of the right to privacy of communications. The constitutional foundation of the right and the additional guarantees put in place developed a legislative framework on this basis. By contrast, in other states, the confidentiality of communications is only a part of the national security and intelligence collection issues. security and intelligence collection issues.

The Greek legislative framework is **formally adequate, in particular because it provides for ex ante control over the lifting by judicial officials. At the same time, it is oriented towards the protection of rights.** In other legal orders, however, it is accepted that the lifting of confidentiality of communications is one of the most secure methods of prevention, in terms of national security, and it is clear that the focus is mainly on electronic communications. With these two facts in mind, controls over the legality of the operation of intelligence services do not focus on the rate and number of cases of lifting - as it is well known that the number is increasing - but on the intelligence service itself. It is in this respect that there are **serious deficiencies in the supervisory authorities and the oversight bodies.** Intelligence collection is the primary objective of the NIS and therefore the oversight on the service should not be limited to the institutional role of the NIS but rather broadened and made more substantial.

Furthermore, the evolving information society, is based on electronic communications and the assessment of personal data. Thus, the **role of data protection authorities needs to be institutionally strengthened.** The multitude of independent authorities active in the field of human rights impose the existence of a comprehensive institutional framework and a more complete legislative provision for their organisation and functioning, as well as for the way in which they interact.

Together with the concluding observations of the Report, the GNCHR highlights the need for transparency in the functioning of the intelligence services. Intelligence services are often involved in highly sensitive and classified activities that cannot be made public and there may be cases where certain information shall not be disclosed to supervisory bodies. Moreover, intelligence services may have a certain level of autonomy in carrying out their activities in order to maintain their operational



efficiency. In any case, the confidentiality surrounding the work of intelligence services and relating to their operational activities is in no way correlated with the lack of reporting and accountability to supervisory mechanisms. Moreover, in the context of the transparency of their operation, it would be useful to publish regular reports on the intelligence services' surveillance activities. These reports could be made public and provide information on the number of surveillance requests, the types of intelligence collected and the number of individuals affected.

The establishment of a mechanism for preventive random controls on the lifting of confidentiality would be an innovative practice towards safeguarding the confidentiality of communications. Such a mechanism could perform preventive random surveillance of communications to ensure that they are indeed secure and private. The mechanism includes procedures that can identify potential security threats and privacy breaches before they occur. These procedures may include regular overights, risk and vulnerability assessments of communication systems and networks. Retrieving communication extracts at intervals may be part of this mechanism operation, in order to ensure that national intelligence services comply with security and privacy policies and standards. In sum, the establishment of a mechanism for conducting preventive random control on the security and confidentiality of communications is a key element of a comprehensive security and confidentiality scheme.

Notifying the person under surveillance in due time after the cessation of the interception is necessary for safeguarding the principle of proportionality. This means that when the interception is no longer necessary, appropriate or proportionate to the objective pursued, the person intercepted should be relatively notified. Providing for a notification of the person under surveillance within a reasonable time after the cessation of the surveillance is useful for a number of purposes. Firstly, it ensures respect for his or her confidentiality and privacy. By notifying the citizen that the surveillance has ceased, it is up to him or her to decide whether he or she wants to take further action to remedy the breach and what to do next. Secondly, it helps to build trust and transparency. Finally, it helps to prevent any unintended consequences or harm that may have resulted from the surveillance. In general, timely and reasonable notification of the person under surveillance after the cessation of surveillance is crucial to ensure that the surveillance is conducted in a proportionate and ethical manner.

The role of the judiciary becomes vital for the rapid investigation of cases where the principle of proportionality in relation to the breach of confidentiality of communications appears not to have been respected. A rapid investigation allows for the imposition of remedial measures but also the cessation of any further intrusive measures, the deletion or destruction of any information obtained illegitimately or without sufficient justification and payment of compensation to individuals affected. Overall, ensuring that the principle of proportionality is respected in the course of investigations is crucial to safeguarding the right to privacy and maintaining public



confidence in the integrity of intelligence services, but also in the justice system and the rule of law in general.

Safeguarding of the constitutional mission of independent authorities, in this case of the Hellenic Authority for Communication Security and Privacy and the Hellenic Data Protection Authority is a necessary condition in order to ensure that they continue to accomplish their tasks "unhindered" by any subsequent legislation that potentially deprives them of their institutional duty, as well as to prevent institutional conflicts such as those arising from the unclear boundaries of supervision and oversight between the judiciary and the independent authorities vis-à-vis the intelligence services. As to the supervisory bodies in particular, their independence lies in the adequacy of their powers of action and responsibilities, especially in relation to the executive, the adequacy of their financial resources and staff (sufficient and properly trained) and the modern technological infrastructure they have in place.

To meet the above objectives, it is further recommended the institutionalisation of the possibility for the independent authority (ADAE) to get personal reports on the lifting of confidentiality from affected persons as well as of the functional interface between the DPA and the ADAE. The functional interconnection among the independent authorities can take various forms. In this regard, independent authorities with delegated powers such as that of the ADAE and the DPA may need to coordinate with each other, to ensure that both the confidentiality of communications and the protection of personal data are not compromised by actions of the State or third parties and in this sense help to strengthen their protection. Under conditions they could exchange information with each other in the context of the effective performance of their tasks or cooperate in order to reach a more comprehensive level of oversight of services under their responsibility.

Special mention should be made of the digitisation of the ADAE archive. The digitisation of the archive includes the conversion of physical files into digital files which can be stored and retrieved electronically. This allows archives to be searchable and easily accessible to authorised personnel via computers or other electronic devices and can help improve efficiency as digitised recordings can be rapidly searched to manage physical archives. Furthermore, digitisation offers both increased accessibility and enhanced security as digital recordings can be protected by encryption and access control, in order to prevent unauthorised access or hacking.

The supervisory mechanisms of the intelligence services, while pursuing their aim, have on several occasions demonstrated their limitations. Their effectiveness in fulfilling their aim may depend on the political will and the resources available. In some cases, oversight may be diminished by political pressure or due to lack of resources, which could jeopardise the ability of supervisory bodies to effectively monitor the intelligence services.

In summary, a delicate balance must be struck between the protection of national



security and safeguarding of individual freedoms, while ensuring that supervisory bodies have the necessary power and resources to fulfil their tasks effectively.

On the other hand, judicial supervision should ensure that the powers of the authority are exercised legitimately and that any interference with the privacy of the individual is necessary and proportionate. The judiciary should also be able to review the decisions of the authority and the intelligence services. Accordingly, the executive is responsible for the operation of the intelligence services. However, such supervision should not unjustifiably interfere with the independence of the authority or compromise its ability to protect confidentiality and security.. Overall, the boundaries among the independent authority and the judicial and executive supervision and oversight on intelligence services should be based on a clear legal framework that provides for effective safeguards for privacy, while ensuring accountability and transparency.

In conclusion, the GNCHR notes that effective supervision of intelligence services is essential to ensure that they operate in a manner consistent with the values of the society they serve and that their activities do not impair individual rights and freedoms. It is a complex and ongoing task that requires constant balancing to ensure that the rule of law is not affected. The institutional framework for control, as reflected in the European legal orders, lacks homogeneity and variations are observed in the relations set up in the national legal orders among independent authorities, the judiciary and the executive. Procedural and substantive guarantees for setting limits to oversight and control exercised by each party over intelligence services can be established through the effective regulation of the legal framework for the confidentiality of communications, a condition that the State has a democratic duty to meet and to which the GNCHR is hereby seeking to contribute. The Commission will continue to closely monitor issues relating to the institutional framework and its harmonisation with the EU and international law so as to safeguard the inviolability of the right to confidentiality of communications, the protection of personal data and to ensure a strong regulatory framework for the control of security and intelligence services.