



SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE
RULE OF LAW ACROSS DEMOCRATIC STATES



The University of Texas at Austin

Strauss
C E N T E R
for International Security and Law

ELECTRONIC SURVEILLANCE IN ROMANIA: LAW, POLICY, AND PRACTICE

Aitana Radu



ABOUT THE AUTHOR



Dr. Aitana Radu is the Security Research Coordinator within the Department of Information Policy & Governance at the University of Malta. Her research focuses on different aspects of security science, from violent radicalisation to intelligence oversight. After a term of service as an operational field officer in the national security sector, Dr Radu spent six years as a researcher in the field of security and intelligence studies for the ‘Mihai Viteazul’ National Intelligence Academy, in Bucharest, Romania where she led the Security Policies Research Unit before taking up a position with the University of Malta. Since 2013, Dr Radu has worked on several European-funded research projects in both the design and implementation phases, focusing mostly on radicalization in the ARMOUR and JP-COOPS projects, law enforcement practices (CITYCoP), the implementation of the European Investigation Order (SAT-LAW and PRE-RIGHTS), developing security science (ESSENTIAL) and intelligence analysis in the MIRROR and CRITERIA projects. Dr. Radu obtained her M.A. (Comparative Political Science) from the University of Bucharest with a thesis on democratic transitions in the Middle East, her M.A. in the Management of Intelligence Activities for National Security from the National Intelligence Academy in Romania with a thesis on the security risks posed by the radical Islamic discourse, and her PhD in Intelligence and National Security from the same Academy with a thesis on the transformation of intelligence organizations. More information and publications at <https://www.um.edu.mt/maks/ipg/staff/aitanaradu>.

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

3	I. Introduction
4	II. Institutions
6	III. Operational Capabilities and Priorities
7	IV. Process for Conducting Surveillance
9	V. Relevant Law
10	VI. Transparency
10	VII. Reforms
12	VII. Other Important Factors

NOVEMBER 2023

I. INTRODUCTION

Romania's intelligence community and intelligence oversight system reflect its recent history and especially its transition from its Communist past. The intelligence system as it currently stands was created in the early 1990s by dividing the former Communist regime's feared Securitate into separate agencies for domestic and foreign intelligence, as well as military intelligence and law enforcement. In the last 30 years, Romanian intelligence agencies have undergone multiple processes of democratization and modernization, but these processes have generally not been reflected in the legislative framework, which remains outdated and patchy.

As such, the Romanian intelligence oversight system is a very weak one, raising considerable doubts as to whether appropriate safeguards are in place when it comes to surveillance. Moreover, in spite of governmental efforts towards increasing transparency of intelligence activities, the topic remains very much outside public scrutiny, with little to no information available on either the technological capabilities of the intelligence agencies or the effectiveness of human rights safeguards.



II. INSTITUTIONS

In the early 1990s, Romania built its new intelligence system by dividing the former Securitate into several agencies which retained the former Communist intelligence system's infrastructure, logistics, personnel, and some source networks, as well as the bulk of its files and archives.

Today, Romania's intelligence-gathering capabilities are shared between three main intelligence agencies and three other directorates with intelligence-gathering capabilities, which are placed under the executive.¹ The first category includes the Romanian Intelligence Service (SRI),² which is the main domestic intelligence service; the Foreign Intelligence Service (SIE);³ and the Protection and Guard Service (SPP),⁴ focused on protecting dignitaries and their relatives.

Other units which are able to request electronic surveillance measures in their respective fields are the General Directorate for Defence Intelligence (DGIA), placed under the Ministry of Defence; the General Directorate for Internal Protection and Intelligence (DGIPI), under the Ministry of Interior; and the National Administration of Penitentiaries (ANP), under the Ministry of Justice. However, out of these last three only the DGIA would fall under the national security umbrella, in the general understanding of the term. The others collect intelligence for criminal investigation purposes and would therefore fall under the provisions of the Criminal Code.

Today, Romania's intelligence-gathering capabilities are shared between three main intelligence agencies and three other directorates with intelligence-gathering capabilities, which are placed under the executive. The first category includes the Romanian Intelligence Service (SRI), which is the main domestic intelligence service; The Foreign Intelligence Service (SIE); and the Protection and Guard Service (SPP), focused on protecting dignitaries and their relatives.

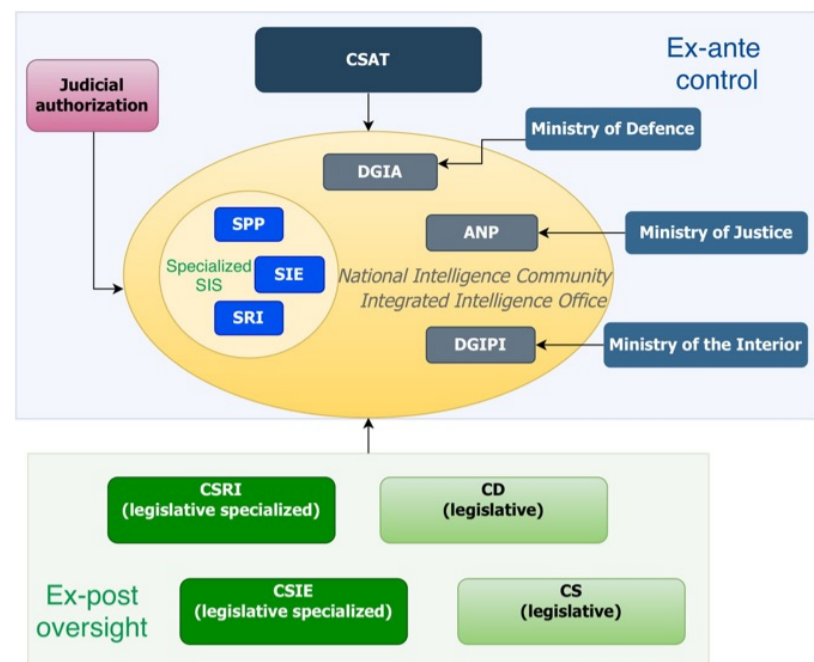


Fig. 1 - Romania's intelligence system.⁵

Requests for electronic surveillance⁶ require judicial pre-authorization. The pre-authorization is a two-step process, in which the request is first assessed by the General Prosecutor of the Prosecutor's Office attached to the High Court of Cassation and Justice, which can either decide to reject the request or forward it to the President of the High Court of Cassation and Justice,⁷ asking in writing for the authorisation of the requested activities.⁸ The request is then examined with urgency in the council room by one of the judges appointed by the President of the High Court of Cassation and Justice. If the judge believes that the request does not include sufficient information, he or she can ask in writing for further information to be submitted. If the judge finds the request justified, then authorisation is given.

At the time of authorisation the judge also issues a National Security Interception Mandate (MSN), which describes the legal basis for the interception. In addition to evidence of a threat, which is required for a MSN to be issued, the intelligence agencies must also include proof that there are no other ways to access that information.⁹

It is important to note that no technical experts take part in the process of judicial authorization. It is also not clear whether the prosecutors and judges involved in the process of assessing requests for surveillance receive any specialized training in this field. The apparent lack of special training raises significant concerns as to the ability of the judicial personnel to accurately review the surveillance requests they receive, more so when considering the process by which law graduates can accede to the position of prosecutor or judge without prior career experience.¹⁰



Unlike many other European countries, Romania does not have a specialized independent agency to oversee intelligence activities. Instead, post hoc oversight is carried out exclusively by the Romanian Parliament through its specialised committees. Unlike the majority of European democratic states, which have only one specialised parliamentary committee, Romania has four, of which two specialize in overseeing the legality of surveillance measures. On the other hand, Romania has no specialised full-time oversight agency comparable, say, to IPCO (Investigatory Powers Commissioner's Office) in the UK, or CTIVD (Review Committee on the Intelligence and Security Services) in the Netherlands.

Two of the parliamentary committees perform substantive oversight of the principal foreign and domestic intelligence agencies. SRI, the domestic service, is overseen by the Joint Standing Committee for the Exercise of Parliamentary Control over the Activity of the Romanian Intelligence Service (CSRI, or "SRI Committee").¹¹

SIE, the foreign service, is overseen by the Joint Standing Committee of the Chamber of Deputies and the Senate for the Exercise of Parliamentary Control over the Activity of the Foreign Intelligence Service (CSIE).¹² Two other committees are responsible for checking the financial expenditures of the two main services: The Committee for Defence, Public Order and National Security of the Chamber of Deputies (CD) and the committee with the same name in the Senate (CS).

Appointment to the four committees is done solely on a political basis, but their members are required on appointment to swear that they have never been members of the former Securitate or employees of a Romanian intelligence agency. The lack of knowledge among their members, coupled with the high rate of changes in their composition, has led some of their own members to criticize the lack of institutional memory and overall inefficiency.¹³

Furthermore, there have been instances where the Romanian press has flagged the appointment of certain politicians because of their professional connections to the Romanian intelligence community.¹⁴ Some of the committees have also come under severe criticism by members of the intelligence agencies themselves. For example, Cristian Maior, the former Director of the Romanian Intelligence Service (SRI), vigorously disputed the SRI Oversight Committee's 2019 finding that the agency used its powers for political purposes during his tenure.¹⁵

In recent years, some of the committees have become more proactive in sharing information. More often than not, however, their site visits to intelligence units seem to be more a case of public communication than real oversight.¹⁶ That being said, most of the debates and presentations before the four committees are closed to the public, with little if any substantive content being made public.¹⁷

When it comes to ex ante control, the Supreme Council of National Defence (CSAT) exerts a certain degree of control over the budget of the intelligence agencies, the development and implementation of the national strategy on national security, and of all legislative projects advanced by Parliament in the field of national security.

The Council also approves the organizational structure and the internal regulations of SRI, SIE, STS and SPP. However, it does not review operations once they have been conducted, a power reserved for the parliamentary committees.

However, upon examining the composition of the CSAT,¹⁸ it is clear that it cannot exercise effective oversight, as the heads of the main intelligence agencies are also members of the Council. The activity of the CSAT itself is subject to Parliamentary Oversight through each house's specialized committee on Defence, Public Order, and National Security. However, as with parliamentary oversight over the intelligence agencies, the control exerted by Parliament is limited to a purely formal exercise, consisting in the presentation of the CSAT's annual report in a closed session in front of the two Chambers.¹⁹

III. OPERATIONAL CAPABILITIES & PRIORTIES

Electronic surveillance²⁰ is mainly carried out by the National Center for Communication Interception (CNIC), which forms part of the Romanian Intelligence Service (SRI). The Center is tasked with collecting, processing, and storing information related to national security.

The collection of data takes places in the centers of telecom providers who then transfer it, in an automated manner, to the system administered by CNIC, without the intervention of a human operator. The CNIC system provides simultaneous, autonomous, and independent access to four interception authorities: the SRI, which operates the system, plus three law-enforcement agencies (the General Prosecutor's Office, the Anti-Corruption Directorate, and the Directorate for Investigating Organized Crime and Terrorism).

The CNIC's legality remains hotly debated. The Center was created by a decision of the Supreme Council of National Defense, not through a law, something which has been recurrently flagged by the Romanian Constitutional Court.²¹

Experts within the Foreign Intelligence Service have publicly asserted that it does not possess electronic surveillance capabilities, instead employing the platform provided by CNIC, as is the case with law enforcement authorities.²²



On the other hand, by law, the General Directorate for Defence Intelligence (DGIA), is allowed to carry out its own electronic surveillance operations both within and outside Romania in order to counter national security threats related to Romania's military. No information about the DGIA's capabilities is available in the public domain, beyond the fact that it possesses SIGINT capabilities and has its own technical equipment for surveillance.²³

■ *The CNIC's legality remains hotly debated.*

Since 2022, the law also empowers agencies to compel companies to help with internet-based collection. Specifically, Law 198/2022 now requires providers of IP-based electronic hosting services²⁴ to assist law enforcement and national security agencies in the execution of electronic surveillance. Under the new law, companies must:

- Allow the legal interception of communications and cover the associated costs for the duration and in the condition mentioned in the authorization documents issued by the judicial authorities;
- Provide the encrypted content of communications shared through their networks;²⁵ and
- Provide access to their own IT systems, for the purpose of replicating and extracting information in accordance with authorization given.²⁶

There is very little confirmed public information related to the proficiency and technologies employed by CNIC. Although there have been some rough estimates as to the total number of employees, the figures have not been officially confirmed.²⁷ Moreover, there is no public information on whether Romanian intelligence agencies currently have the technological capability to carry out bulk surveillance, nor are there provisions related to this in the current legal framework.²⁸

The priorities for intelligence collection are established in an official document submitted annually by the National Intelligence Community,²⁹ which is then sent for approval to the Supreme Council of National Defence (CSAT), and finally to the President. The document identifies the main risks, threats, and vulnerabilities to national security and aims to ensure effective planning of all intelligence activities.

IV. PROCESS FOR CONDUCTING SURVEILLANCE

Romanian law does not distinguish between domestic and overseas targets of surveillance; therefore, the process outlined below applies to both cases.

All requests for electronic surveillance follow the same authorization process. Under the law on national security,³⁰ the intelligence agency seeking to employ electronic surveillance methods submits an authorisation request to the General Prosecutor of the Prosecutor's Office attached to the High Court of Cassation and Justice. The prosecutor is required at this stage to carry out the legality, necessity, and proportionality test and can either reject the request or forward it to the President of the High Court of Cassation and Justice,³¹ asking in writing for the authorisation of the requested activities.³²

The request is then examined by one of the judges appointed by the President of the High Court of Cassation and Justice. If the judge considers that the request does not include sufficient information, he or she can ask in writing for further information to be submitted. If the judge considers that the request is justified, then authorisation is given. At this time, the judge also issues a National Security Interception Mandate. The duration of the authorisation cannot be longer than 6 months. The authorisation can be extended with the same conditions, for valid reasons, but the extension cannot be longer than 3 months. The maximum duration of an authorisation for the same set of evidence justifying the existence of a national security threat is 2 years.

If the judge finds that the request is not justified, then the request is rejected. A new request regarding the same person can only be requested and granted if the request is based on new information.

Authorisation can also be granted in emergency situations by the prosecutor for a duration of 48 hours, provided that the judge's authorisation is requested as soon as possible, but not before the initial authorisation expires. In this situation the judge is required to immediately analyse the request and give a decision.

As for collection outside Romania's borders, the Foreign Intelligence Service (SIE) has denied on multiple occasions that it has the technical capacity to carry out electronic surveillance itself, arguing that all its surveillance requests are implemented through the CNIC.³³ Furthermore, Law 1/1998 also states that intelligence collection, validation, and exploitation activities must not in any way harm the fundamental rights and liberties of Romanian citizens; their private life, honour, or reputation; or subject them to any illegal limitations. This provision does not, however, refer to foreign citizens, which would seem to indicate that this latter category would be legitimate targets of electronic surveillance by SIE without necessarily deploying the same level of safeguards as would be required for Romanian citizens.

When it comes to the military intelligence service (DGIA), its surveillance activities target both internal and external threats, following the same process outlined in Law 51/1991.

Although in theory there seems to be an a priori oversight mechanism in place, the effectiveness of the system has been challenged by legal experts. Namely, according to an analysis carried out by a private law firm, in the period from 2009 to 2018, over 26,000 electronic surveillance national security mandates were approved, with an average of 4,000 per year, out of which only two requests were rejected during the entire period.³⁴ This raises some doubts as to the rigor of the legality, necessity, and proportionality assessment carried out by the prosecutors and judges involved in the authorization process.³⁵

V. RELEVANT LAW

Constitutional Limitations

There are no constitutional limitations, except for the provisions related to the right to privacy (Article 26 of the Romanian Constitution). It is important to note, however, that all provisions of the Romanian Constitution must be interpreted in compliance with the jurisprudence of the European Court of Human Rights, which has produced considerable case law related to surveillance.

Statutory Limitations

The main legal instruments applicable for electronic surveillance for national security purposes are the following:

1. Laws defining the sphere of national security and describing the process for employing electronic surveillance:
 - Law 51/1991 on Romanian national security.³⁶ This is the fundamental law in the field of national security, listing all the threats³⁷ that fall under the national security umbrella, and which therefore may justify the use of intelligence means (including electronic surveillance). The law also describes in detail the procedure required for using electronic surveillance methods. The provisions of Law 51/991 must be analyzed in conjunction with the jurisprudence of the Romanian Constitutional Court, namely Decision 91 from 28th February 2018 and Decision 51 from 16th February 2016, which brought several changes to the law.
 - Law 535/2004 on the prevention and combating of terrorism,³⁸ which was adopted after the 9/11 terrorist attacks in the US and further expanded the use of electronic surveillance.

- Law 198/2022 for the amendment and completion of normative acts in the field of electronic communications and for the establishment of measures to facilitate the development of electronic communications networks. This law has also further expanded the use of electronic surveillance to cover IP-based electronic hosting services.
2. Laws on the organization and functioning of the various intelligence agencies,³⁹ which introduce the specific national security area covered by each agency as well as the extent of powers and safeguards associated with each intelligence agency.

While Law 51/1991 limits the purposes for which Romanian intelligence agencies may conduct electronic surveillance to the 13 national security threats listed in footnote 38, *supra*, in practice, there has been quite a lot of overlap between the use of electronic surveillance by intelligence agencies for national security purposes and the use of electronic surveillance by intelligence agencies⁴⁰ as part of criminal investigation proceedings in relation to national security threats.

The problem has been further compounded by the loose and often conflicting interpretation given to the term “national security threat” by various bodies active in the field. Romanian law has struggled to delineate between “national security” threats assigned to the intelligence agencies and purely criminal matters. In its most recent decision on the subject, the Constitutional Court held that activities linked to national security focus on identifying, preventing, and countering internal and external threats to national security, while criminal investigation activities focus on bringing to justice individuals who have committed crimes.⁴¹ That holding builds on a previous decision holding that in cases falling under the Criminal Code, only criminal investigative authorities and prosecutors can use surveillance methods.⁴² The end result was to prohibit the domestic intelligence service (SRI) from providing assistance to criminal investigative authorities in executing surveillance operations,⁴³ even when the crimes in question would fall under the framework of national security.

Romania also subscribes to the Council of Europe's Convention 108⁴⁴ the European Convention on Human Rights, which means it must also adhere to the Convention's human rights safeguards in conducting electronic surveillance. In several instances, the European Court of Human Rights has found Romania in breach of its obligations in relation to activities carried out by its intelligence agencies.⁴⁵

VI. TRANSPARENCY

Romania offers relatively little transparency about its electronic surveillance in the field of national security.

While all laws related to national security and the activity of intelligence agencies are publicly available, that is largely the extent of public information available on this subject. And Parliament has frequently approved changes to these laws with little or no public debate.⁴⁶

Given the central role which the domestic intelligence service (SRI) has in carrying out electronic surveillance,⁴⁷ most of the information available on this topic can be extracted from its annual reports, which are approved by Parliament and then published in the Official Monitor and on the organization's website. However, these reports are often published with significant delay⁴⁸ and they only contain vague data regarding SRI's surveillance activities.⁴⁹ In the past, the reports included more detailed information on the number and types of national security mandates that had been authorized, but the more recent ones no longer include such information. In the case of SIE, the foreign intelligence service, its annual reports are not made public; instead, they are presented only to the CSAT. Similarly, there is no information in the public domain on the electronic surveillance activities of the defense intelligence service (DGIA).

The lack of a vibrant civil society focused on the protection of fundamental rights means that there are also very few independent experts and entities that carry out lobbying and advocacy activities in the field.

Unfortunately, the parliamentary oversight bodies' public statements and reports add little insight into electronic surveillance issues. Often, they simply provide a summary report of their own oversight activity and express their satisfaction with the work carried out by the intelligence agencies without providing any concrete information.

Furthermore, most decisions about intelligence priorities, budget allocation, and infrastructure are discussed and approved within CSAT meetings. As the minutes of these meetings typically are classified, very little public information is available. Although the CSAT is required to publish annual reports of its activity, these reports are published with significant delay.⁵⁰

The lack of a vibrant civil society focused on the protection of fundamental rights means that there are also very few independent experts and entities that carry out lobbying and advocacy activities in the field.

VII. REFORMS

Given the outdated and patchy character of Romanian legislation in the field of national security, there have been multiple attempts at reform since the country's transition towards democracy. However, due to the lack of political consensus coupled with a proportionate lack of public outcry, these attempts have mostly been unsuccessful. Overall, this has led to a situation in which the current legislative framework neither ensures that intelligence activities are carried out in an efficient manner nor provides robust human rights safeguards.

In this context, and considering the deteriorating security environment around Romania, in June 2022, the government proposed a series of laws to address gaps in the field of security.⁵¹

The most important proposed changes are the following:

- A significant extension of the sphere of “national security” for purposes of electronic surveillance: The term would now include organized crime, as well as malicious actions that target the administrative, health, educational, cultural heritage, critical infrastructure, communications, and ICT sectors, as well as national financial, economic, energy, and research interests. Such an extension would enable electronic surveillance measures to be used in these areas by SRI and other intelligence agencies, not merely by criminal authorities.
- Changes to the surveillance authorization procedures: SRI would be able to submit its authorization requests directly to the High Court of Justice and Cassation, without having to undergo the assessment of the General Prosecutor’s Office.
- Changes to the oversight mechanisms: Though Parliament would continue to oversee the SRI, the agency would no longer be required to present its annual report in front of Parliament; this obligation would be transferred solely to the specialized oversight committees in Parliament.
- Changes related to the CNIC: The CNIC’s role in electronic surveillance would be codified, potentially addressing the criticism raised by the Constitutional Court as to the legality of the CNIC.
- Changes to the spheres of action of SRI and SIE: SRI would be given the power to also act abroad if the actions are closely linked to a domestic threat to national security, while SIE would be given the power to also act domestically if the threat is linked to foreign entities.

It is not clear at the time of writing (October 2022) whether the laws will be adopted and in what form.⁵² While the need to modernize the legal framework is real, the way the laws were drafted⁵³ and made public led to a significant public outcry. Moreover, due to the negative associations between intelligence and the former Communist regime, there is significant societal distrust and reluctance to award more powers to security institutions.



If enacted, these changes would weaken oversight while expanding the powers of intelligence agencies beyond what is the current norm in other European countries. For example, the review process for surveillance authorization procedures, already weakened by the absence of technical experts or intelligence specialists, would be further enfeebled by the replacement of the double review (Prosecutor and Judge) with a single review (Judge only). As a result, even fewer experts would be involved in the authorization process. At the same time, placing the full oversight burden solely on the specialized oversight committees would be another sign of weakness, given the lack of knowledge and inefficiency of these committees outlined in the previous sections.

The extension of the spheres of actions of SRI and SIE would be particularly problematic, especially given the outdated and imprecise phrasing of Law 51/1991. This could enable the extension of the national security umbrella over a wide range of societal issues and over an increasingly weakened oversight system.⁵⁴

VIII. OTHER IMPORTANT FACTORS

Romania's Communist past remains a defining element when trying to understand both how its intelligence community functions and the relationship between the state, security agencies, and the general public. Since 1989, there have been multiple waves of reforms aimed at democratizing and modernizing Romania's intelligence community, especially in the context of its integration into NATO and the EU. Experts agree, however, that the move has been "more towards effectiveness and less towards accountability and democratic control."⁵⁵

Another important element is that the legal framework (Law 51/1991), which is supposed to provide a foundation for Romania's intelligence activities, was adopted immediately after the fall of the Communist regime and has undergone few changes to this day. To compound the problem, both SRI and SIE started to operate before their legal status was even clarified.⁵⁶ The fact that all of these laws were adopted in the 1990s, when Romania was still in the early stages of its transition to democracy, with many of the former intelligence elite still active in the agencies themselves, explains to a certain extent why the human rights safeguards introduced were so weak.

Moreover, because the main intelligence agencies are direct heirs of the ruthless Securitate, which was responsible for both domestic repression and foreign espionage, they still face a serious deficit of public trust. Multiple scandals related to politicization of intelligence, disclosure of classified information, and abuse of power (especially in the 1990s and early 2000s), coupled with an overall lack of transparency regarding their activities, has harmed their public image.

Romania also holds a strategic position at the borders of the EU and NATO, a complex security environment that poses significant pressure on the Romanian intelligence community. In this context, a reform of the security and intelligence legislation is much needed.

That being said, the public opinion barometers published in the last years indicate that the public trust in SRI, the Ministry of Foreign Affairs, or the Army is higher than that in other public institutions, such as Parliament, Government, or even the Orthodox Church.⁵⁷ However, when the new draft laws on security issues were published earlier in 2022, it was clear that the public is still very reluctant to grant more powers to intelligence organizations. The overwhelming reporting on the subject indicated a complete distrust of human rights safeguards in place when it comes to surveillance operations.

Romania also holds a strategic position at the borders of the EU and NATO, a complex security environment that poses significant pressure on the Romanian intelligence community. In this context, a reform of the security and intelligence legislation is much needed. On the one hand, this would ensure that intelligence agencies are able to meet national and regional requirements in the context of a volatile security environment. On the other, it would be an opportunity for stronger human rights safeguards.

Unfortunately, the focus of the new draft laws on security has not been on strengthening intelligence oversight. Romania should align itself with international best practices in the field by creating an independent expert body (including both legal and technical experts) that would carry out both a priori and a posteriori review of surveillance operations.

Furthermore, lawmakers should create stronger remedial mechanisms that would enable citizens who feel they have been the target of unjust surveillance measures to seek justice through appropriate remedies.⁵⁸ The creation of such bodies would not only strengthen the oversight system but would also increase transparency in the field. In the long run, this would foster a positive debate on intelligence issues within Romanian society.

ENDNOTES

1. In addition to these, there is also the Special Telecommunications Service (STS), which organizes and coordinates telecommunications activities for the public authorities in Romania and for other users in accordance with the law. The institution also provides national signals intelligence (SIGINT). As no further information beyond this is available in the public sphere, it is safe to assume that STS mainly specializes in communications infrastructure and security, while interception is mainly covered by the Romanian Intelligence Service. Florina Cristiana Matei, *Romania's anti-terrorism capabilities: transformation, cooperation, effectiveness*, 3 Journal of Defense Resources Management (2012), <https://link.gale.com/apps/doc/A338602934/AONE?u=googlescholar&sid=bookmark-AONE&xid=d471f754>, accessed on 28th September 2022.
2. Law no. 14 from 24 February 1992 on the organisation and functioning of the Romanian Intelligence Service.
3. Law no. 1/1998 on the organisation and functioning of the Foreign Intelligence Service.
4. Law no. 191/1998 on the organisation and functioning of the Protection and Guard Service.
5. T. Cotarcea, *Towards a coherent information policy in intelligence oversight: a comparative approach to emerging trends*, Master by Research Dissertation in Information Policy and Governance, University of Malta (2019).
6. It is important to note that the Romanian legislative framework does not distinguish between real-time and stored communications, wire and radio communications, or telephony and IP-based communications.
7. The prosecutor has 24 hours to carry out the analysis, which starts from the moment when the request was registered with the Prosecutor's Office. The analysis can be carried out immediately in emergency situations, by prosecutors specifically appointed by the General Prosecutor of the Prosecutor's Office attached to the High Court of Cassation and Justice for this very purpose.
8. "In *Popescu v. Romania*, the [European] Court [of Human Rights] considered that the Romanian authority which ordered the surveillance (the prosecutor) was not independent from the executive. It stated that the authorising body must be independent and that there should either be judicial control or independent control over the issuing body's activity. Similarly, in both the *Iordachi* and the *Association for European Integration and Human Rights* and *Ekimdzhiiev* cases the [same] Court stressed that independent controls should exist at both the authorisation stage and the follow-up stage. The [European] Court [of Human Rights] has a preference for judicial authorisation, even if, in *Kennedy v. the United Kingdom*, it accepted the British system of ministerial authorisation." Council of Europe, *Mass surveillance – who is watching the watchers?*, at para. 106 (2015); see also Council of Europe, Venice Commission, *Democratic and Effective Oversight of National Security Services* (2015), <https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb>, accessed on 3rd September 2022.
9. Revista Intelligence, *Mandatul de securitate națională* [The national security mandate], 6 October 2015, <https://intelligence.sri.ro/mandatul-de-securitate-nationala/>.
10. Under the Romanian legal system, a law graduate can directly opt to take the Magistrate exam, which gives them access to a special school for graduates who want to become judges or prosecutors.
11. Romania, Decision no. 30/1993 of the Romanian Parliament concerning the Organization and Functioning of the Joint Permanent Commission of the Senate and the Chamber of Deputies for the Exercise of Parliamentary Control over the Activity of the Romanian Intelligence Service, 23 June 1993.
12. Romania, Decision no. 44/1998 of the Romanian Parliament concerning the Organization and Functioning of the Joint Permanent Commission of the Senate and the Chamber of Deputies for the Exercise of Parliamentary Control over the activity of the External Intelligence Service, 28 October 1998.
13. In 2022, one of the MPs appointed to the SRI Committee argued in an interview that it takes a committee-member at least a year to understand its basic organisation, and a whole term to understand not only the legislation in the field but also the mode of interaction. Emilian Isailă, *Deputat din Comisia SRI: Mă îngrijorează logica nedemocratică ce a stat la baza drafturilor legilor securității – Interviu* [Deputy from the SRI Commission: I am worried about the undemocratic logic that was the basis of the draft security laws – Interview], SpotMedia.ro, 11 July 2022, <https://spotmedia.ro/stiri/politica/deputat-din-comisia-sri-ma-ingrijoreaza-logica-nedemocratica-care-a-stat-la-baza-drafturilor-legilor-securitatii-interviu>.
14. For example, one of the members of the SRI Committee appointed in 2020 had completed 3 postgraduate courses (one at the Ministry of Foreign Affairs, one at the Defense College of the Ministry of Defense, and another at the Internal Affairs College of the Ministry of Foreign Affairs) and a Doctoral degree at institutions directly affiliated with the intelligence community.
15. G4Media.ro, *George Maior cere desecretizarea integrală a audierilor din Comisia SRI / Ce spune despre acuzele de poliție politică* [George Maior demands full declassification of the hearings from the SRI Commission / What he says about the accusations of political police], 27 April 2019, <https://www.g4media.ro/george-maior-cere-desecretizarea-integrala-a-audierilor-din-comisia-sri-ce-spune-despre-acuzele-de-politie-politica.html>.
16. The Committee responsible for overseeing SRI has published on its Facebook account summaries of the visits it has carried to all 11 regional intelligence units. However, it is clear from the information provided that the visits were a public communication exercise,

with no substantive matter being reported. See the Committee's Facebook account, "Comisia parlamentară pentru controlul activității SRI," at <https://www.facebook.com/ComisiaSRI/>.

17. For example, in 2021 the Committee responsible for overseeing SRI has adopted without a real debate five pending SRI annual activity reports, covering the period from 2015 to 2019. The President of the Committee stated at the time that "the Committee concluded that in carrying out intelligence activities, the Romanian Intelligence Service respected the Romanian Constitution and all other laws." Luminita Pirvu, *Cât de controlate de Parlament sunt SRI și SIE / Csoma: Nu vă pot spune pentru că aș putea divulga secrete de stat / Drulă: Mai degrabă SRI conduce comisia decât invers* [How controlled by the Parliament are SRI and SIE / Csoma: I can't tell you because I could divulge state secrets / Drula: Rather SRI leads the commission than the other way around], HotNews.ro, 27 June 2022, <https://www.hotnews.ro/stiri-politic-25640745-cat-control-exercita-parlamentul-asupra-serviciilor-secrete.htm>.

18. The CSAT includes the following members: the President and Prime Minister of Romania; the Ministers of National Defence, Internal Affairs, Foreign Affairs, Justice, the Economy, and Public Finance; the Directors of the domestic and foreign intelligence services; the Chief of the General Staff; and the Presidential Advisor for National Security.

19. The report is then subject to a vote, which is again a purely formal procedure. Only once, in 2006, did members of the Opposition argue against voting for the CSAT report. In that case, they opposed the 2005 report because it proposed to create the Intelligence Community without a previous amendment of Law no. 415/2002. That proposal was not carried out.

20. This presumably covers both telephony-based communications and IP-based communications.

21. CNIC was created through a CSAT decision from 17 July 2002. The Constitutional Court wrote that, with respect to electronic surveillance as regulated by the Criminal Code, the mere reference to an institution/entity meant that to technically execute the authorizations, in the absence of a legal framework, would not be in compliance with the legality principle. Therefore, the creation of the Centre should be provided for by law, which would also regulate its legal status, internal architecture, and competences. However, it appears unlikely that the Court will take further action to effectuate this statement, at least absent other changes to core laws governing national security. Decision no. 55 (16 Feb. 2022), https://www.cdep.ro/pls/legis/legis_ppck.htm?act?ida=184589.

22. The same applies for the dignitary protection service (SPP), whose statute states that all interceptions shall be conducted with the technical assistance of SRI, the principal domestic intelligence service.

23. The agency has its own capabilities but also has access to NATO SIGINT capabilities. DGIA, *Infosfera*, Anul I, no. 3 (2009), https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2009/3_2009.pdf.

24. Law no. 198/2022. This is defined in the law as entities, which on the territory of Romania, provide services related to the storage, distribution, and access to content on their own or on rented servers, by managing a set of IP addresses on the Internet. As the law does not exclude foreign companies, such as Google or Facebook, from its scope, it would appear that as is the case in other jurisdictions, such as Germany or the Netherlands, foreign companies, especially those with local offices, would prima facie be subject to the law.

25. Since nothing is excluded, one can presume that all types of communications are included in the scope of the law.

26. Law no. 198 of 6 July 2022 (for the amendment and completion of normative acts in the field of electronic communications and for the establishment of measures to facilitate the development of electronic communications networks).

27. This has been estimated at around 1,000 employees according to one media source, which is quoting a statement from an SRI expert, which would indicate quite a large organisation, given the size of Romania. Flux 24, *SRI a dat un MILIARD de euro pe serverele de interceptare ale convorbirilor telefonice* [SRI gave a BILLION euros on the interception servers of telephone conversations], <https://flux24.ro/scandalos-sri-a-dat-un-miliard-de-euro-pe-serverele-de-interceptare-ale-convorbirilor-telefonice/>, last visited 15 October 2022.

28. Quite the contrary, the authorization requests for electronic surveillance require multiple identification elements for the individuals, who are the targets of such requests.

29. The National Intelligence Community (CNI) is part of the Supreme Council for National Defense (CSAT) and is composed of the Presidential Councillor for National Security, Director of SRI, Director of SIE, Ministry of National Defense, Ministry of Foreign Affairs, Ministry of Internal Affairs, Ministry of Justice, and Prime Minister's Councillor for Security Affairs.

30. Law no. 51 from 29 July 1991 (on Romanian national security).

31. The prosecutor has 24 hours to carry out the analysis, which starts from the moment when the request was registered with the Prosecutor's Office. The analysis can also be carried out immediately in emergency situations by prosecutors specifically appointed by the General Prosecutor of the Prosecutor's Office and attached to the High Court of Cassation and Justice for this very purpose.

32. "In *Popescu v. Romania*, the Court considered that the Romanian authority which ordered the surveillance (the prosecutor) was not independent from the executive. It stated that the authorising body must be independent and that there should either be judicial control or independent control over the issuing body's activity. Similarly, in both the *Iordachi* and *Association for European Integration and Human Rights* and *Ekimdzhiiev* cases the Court stressed that independent controls should exist at both the authorisation stage and the follow-up stage. The Court has a preference for judicial authorisation, even if, in *Kennedy v. the United Kingdom*, it accepted the British system of ministerial authorisation." Council of Europe, *Mass surveillance – who is watching the watchers?*, at para. 106 (2015); see also Venice Commission, *Democratic and Effective Oversight of National Security Services*, Council of Europe (May 2015), <https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb>.

33. In 2007, the Head of SIE clearly stated that while the Foreign Intelligence Service does carry out electronic surveillance, it does so by using the capabilities provided by the Romanian Intelligence Service. Source: *Săftoiu: SIE ascultă telefoanele, dar prin SRI* [Săftoiu: SIE listens to the phones, but through SRI], *adevarul.ro* (15 March 2007), <https://adevarul.ro/stiri-interne/evenimente/saftoiu-sie-asculta-telefoanele-dar-prin-sri-745271.html>, last visited on 15 September 2022. There is no newer information available to indicate this is not

still the case in 2022.

34. It is important to note that the review cited here covers the period before the two landmark decisions of the Constitutional Court, so it may be the case that the mandates in question referred both to national security mandates as part of domestic and foreign intelligence operations and to national security mandates as part of criminal investigations.

35. *Mandatele de supraveghere în domeniul securității naționale dincolo de statistică* [National security surveillance mandates beyond statistics], Mareș & Mareș (June 9, 2020), <https://mares.ro/2020/06/09/mandatele-de-supraveghere-in-domeniul-securitatii-nationale-dincolo-de-statistica/>. A similar situation was encountered during the first 11 months of 2021, when the High Court of Justice and Cassation had a 0.39% rejection rate of authorizations for national security mandates. Sorina Matei, *EXCLUSIV. Haos la Curtea Supremă de Justiție pe mandatele de Securitate națională din România din 2021* [EXCLUSIVE. Chaos at the Supreme Court of Justice on the National Security mandates in Romania from 2021], MediaFAX.ro (9 February 2022), <https://www.mediafax.ro/justitie/exclusiv-haos-la-curtea-suprema-de-justitie-pe-mandatele-de-securitate-nationala-din-romania-din-2021-20512623>.

36. See Law no. 187/2012 (implementing Law 286/2009 on the Criminal Code); Decision of the Constitutional court no. 91 (28 February 2018) (declaring the unconstitutionality of article 3, letter f from Law 51/1991); Law 2/2016 (adding new subsection “m” to article 3).

37. The list of national security threats includes the following: actions aimed at undermining the sovereignty, unity, or independence of the Romanian state; actions helping a foreign power plan war against Romania; treason; violent actions aiming at weakening state power; espionage or transfer of state secrets to a foreign power or organization; illegal procurement and retention of secret state documents or data with a view to transferring them to a foreign power; disclosure of state secrets or negligence in their keeping; actions that have a purpose to remove by force the democratic institutions of the state or that gravely harm the fundamental rights and freedoms of Romanian citizens, may damage the defence capacity, or other similar interests of the country; acts of destruction, degradation, or bringing in an unusable state the structures necessary to the good development of social and economic life or to the national defence; actions by which an attempt is made on the life, physical integrity, or health of persons holding important positions in the state, or of the representatives of other states, or of international organizations while in Romania; supporting totalitarian or extremist actions of a communist, fascist, “iron guardist,” or of any other origin, of racial, anti-Semitic, revisionist, or separatist actions that can endanger in any way the unity and territorial integrity of Romania (including the instigation of deeds that can endanger the rule of law); planning or supporting terrorist acts; theft of weapons or dangerous materials from units authorized to hold them, or illegal production of these materials; the carrying of weapons or ammunition, without right, if this endangers national security; conspiracies to carry out any of these activities; and actions that harm the strategic economic interests of Romania, including actions that illegally jeopardize or destroy natural resources.

38. The law was recently updated through Law no. 58/2019, with no impact, however, on the issue of electronic surveillance. The changes mainly tackled content removal and a restructuring of the national system for the prevention and countering of terrorism.

39. See Law no. 14/1992 on the organization and functioning of the Romanian Intelligence Service; Law no. 1/1998 on the organization and functioning of the Foreign Intelligence Service; Law no. 191/1998 on the organization and functioning of the Protection and Guard Service; and Law no. 346/2006 on the organization and functioning of the Ministry of National Defense.

40. This refers mainly to the Romanian Intelligence Service.

41. Decision no. 91/2018.

42. Decision no. 51/2016.

43. The use of SRI undercover investigators and intelligence officers as well as a number of other covert actions undertaken by SRI is still permitted under the Criminal Code in criminal investigations dealing with national security threats and/or terrorism. Therefore, the Court’s decision mainly eliminates the use of interception methods and technologies (i.e., electronic and technical surveillance).

44. Romania also signed Convention 108+ in March 2022.

45. Among the cases directly involving Romanian intelligence agencies are the following: *Rotaru v. Romania* – 28341/95 (violation of his right to private life by the Romanian Intelligence Service); *Muhammad and Muhammad v. Romania* – 80982/12 (expulsion on national security grounds decided by court on the basis of classified information not disclosed to applicants, without sufficient counterbalancing safeguard); *Corneschi v. Romania* – 21609-16 (fair proceedings challenging withdrawal of security clearance and decision to discharge applicant from office); *Bucur v. Romania* – 40238/02 (unjustified government surveillance of citizens).

46. Romanian independent experts expressed their concerns on how Law no. 198/2022, aimed to transpose the EECC Directive into national legislation, was passed; , the final legislation included additional provisions detailing the obligations of communication services providers in relation to national security, which had not been included in the Directive and which were not subjected to a public debate.

ApTI, *Romania uses the EECC Directive implementation to extend communication surveillance*, EDRi20 (December 15, 2021), <https://edri.org/our-work/romania-extends-communication-surveillance/>.

47. SRI carries out the electronic surveillance for both SPP and SIE.

48. The most recent one available is from 2019. The reason for the delay is that the annual reports must be approved by the Romanian Parliament, and only after this approval is given can they be published in the Official Monitor and on the website of the institution.

49. This data mainly consists of the total number of national security mandates executed by SRI during that year. For example, in 2019 the total number was 1,170. *Raportul de Activitate Al Serviciului Român de Informații* (2019), at 21, available at <https://sri.ro/rapoarte-de-activitate> (last visited June 15, 2023). The same global numbers can also be obtained from the General Prosecutor’s Office or the High Court of Justice and Cassation, which are the entities tasked at law with assessing and authorising requests for electronic

surveillance.

50. The last annual report available is from 2015.

51. The proposal included 10 draft laws, among which the most relevant for the topic of surveillance were the new draft laws for the organization and functioning of SRI, SIE, and SPP, as well as the draft law on the organisation of intelligence and counterintelligence activities. Cristian Pantazi, *EXCLUSIV G4Media publică integral cele 10 proiecte de legi ale securității naționale – DOCUMENTE* [EXCLUSIVE G4Media publishes the 10 draft national security laws in full – DOCUMENTS], G4Media.ro (3 June 2022), <https://www.g4media.ro/exclusiv-g4media-publica-integral-cele-10-proiecte-de-legi-ale-securitatii-nationale-documente.html>.

52. The Parliamentary debate on the laws was scheduled to begin sometime in late autumn 2022.

53. According to statements made by the Romanian Prime Minister, the laws were drafted by the security agencies themselves.

54. While this is something that would cause strong public controversy outside Romania, in Romania there was limited media coverage of the proposals, and the debate was more focused on the proposals being published without the consultation of different stakeholders than on their substance.

55. Florina Cristiana (Cris) Matei, *Balancing Democratic Civilian Control with Effectiveness of Intelligence in Romania: Lessons Learned and Best/Worst Practices Before and After NATO and EU Integration, Intelligence and National Security*, 29 *Intelligence and National Security* 619, 621 (2014).

56. It is important to note that Law no. 14 (providing a legal framework for SRI) was only adopted in 1992, while Law no. 1 (providing the same for SIE) was not adopted until 1998.

57. This assessment, however, refers more to their effectiveness than to their ability to safeguard human rights. Ramona Rotaru, *Barometru de securitate a României! Cum văd românii lucrurile legate de politică și cum stau cu încrederea* [Romania's security barometer! How Romanians see things related to politics and how they feel about trust], evz.ro (18 October 2021), <https://evz.ro/barometru-de-securitate-a-romaniei-cum-vad-romanii-lucrurile-legate-de-politica-si-cum-stau-cu-increderea.html>.

58. Currently, citizens can lodge their complaints with either the Parliamentary oversight bodies or the courts. However, the burden of proof relies on the citizens, which makes this mechanism very weak and inefficient.