DIRECTORATE GENERAL
HUMAN RIGHTS AND RULE OF LAW

DIRECTORATE OF HUMAN RIGHTS

DEPARTMENT FOR THE EXECUTION OF JUDGMENTS
OF THE EUROPEAN COURT OF HUMAN RIGHTS

H/Exec(2016)6 – 20 October 2016

Case of *Bucur and Toma*[1] v. Romania

Assessment of the legal framework concerning secret surveillance activities based on national security considerations

Memorandum prepared by the Department for the Execution of Judgments of the European Court of Human Rights.

The opinions expressed in this document are binding on neither the Committee of Ministers nor the. European Court.

EXECUTIVE SUMMARY

The problem of the lack of safeguards in Romanian legislation concerning secret surveillance activities in cases involving presumed threats to national security arose in the cases of Rotaru v. Romania, Association "21 December 1989" and Others v. Romania and Bucur and Toma v. Romania, as well as in the Dumitru Popescu (No. 2) group of cases. The Committee of Ministers is currently examining the measures adopted and/or envisaged by the authorities to address this problem within the supervision of the execution of the Bucur and Toma judgment. Substantial changes to the legal framework in question were made by Law No. 255 of 1 July 2013, which entered into force on 1 February 2014. These changes had previously been the subject of discussions between the Department for the Execution of Judgments and the Romanian authorities, which incorporated into the final version of the Law a number of amendments inspired by those discussions. ***Overall, these changes are encouraging as they enshrine key safeguards for the respect of citizens' private life****.*

However, ***a number of shortcomings in the initial legal framework identified by the European Court still need to be addressed****. In order to meet the requirements arising from the relevant case law of the Court, it will in particular be necessary:*

- *to review the mechanism for oversight of the activities of the intelligence services, in order to determine the measures required to ensure its independence and effectiveness;*
- *to clarify the issues related to the categories of persons who may be subject to secret surveillance activities and the type of data that may be collected by the intelligence services as a result of those activities;*
- *when the notification of the person affected by secret surveillance activities has been delayed for one of the reasons authorised by law, to ensure that the intelligence services carry out that notification as soon as those reasons cease to exist.*

[1] Judgment of 8 January 2013, final on 8 April 2013.

*In addition, in order to have a complete and precise picture of the legal framework currently applicable in this area, the authorities should provide **supplementary information** on:*

- *the provisions applicable to the examination, use and retention of data gathered as a result of secret surveillance activities and on the circumstances and procedures to be followed to destroy them;*
- *the provisions applicable to access by the person charged with deeds or actions that jeopardise national security (or his/her representative) to the original carrier of the data collected by the intelligence services;*
- *the legal remedies that can be used to obtain redress by individuals who consider themselves wronged by secret surveillance activities based on national security considerations.*

Contents

I. INTRODUCTION

1. All the cases concerning this issue call into question the activities of the Romanian Intelligence Service[2] (*Serviciul român de informaţii*, hereinafter "SRI"). The Court noted that the legal basis of those activities was Law No. 51/1991 on national security and Law No. 14/1992 governing the organisation and operation of the SRI (hereinafter "Law No. 51/1991" and "Law No. 14/1992"). It held that this legislation did not meet the requirements of a "law" within the meaning of Article 8 of the Convention since it lacked the required safeguards against arbitrary action owing to:

- the absence of provisions on the type of information that may be recorded, the categories of persons who may be subjected to secret surveillance activities, the circumstances in which such activities may be carried out and the procedure to be followed in order to be able to gather, record and archive information concerning national security;[3]
- the lack of independence of the authority that could authorise secret surveillance activities (the public prosecutor) and the absence of limits to the public prosecutor's powers in this area (as the law did not provide for an overall limit on the duration of the surveillance activities);[4]
- the absence of a limit on the age of information held and the length of time for which it may be retained, and the lack of details on the circumstances in which information obtained through secret surveillance must be destroyed;[5]

---

2 The other state authorities with powers in the area of national security are the Foreign Intelligence Service, the Protection and Escort Service and the special agencies of the Ministry of Defence, the Ministry of the Interior and the Ministry of Justice.

3 *Rotaru* [GC], judgment of 4 May 2000, § 57.

4 *Dumitru Popescu (No. 2),* judgment of 26 April 2007, final on 26 July 2007, §§ 70-71.

5 *Rotaru*, cited above, § 57; *Dumitru Popescu (No. 2)*, cited above; §§ 78–79, *Association "21 December 1989"*

- the lack of safeguards to ensure that information obtained through secret surveillance is destroyed as soon as it is no longer necessary in order to achieve the intended objective;[6]
- the lack of legal remedies available to those affected by these measures;[7]
- the lack of oversight procedures, whether while the measure ordered is in force or after it has ceased,[8] and, in this connection, the ineffectiveness of the parliament's oversight of the activities of the SRI;
- the lack of safeguards to ensure that the original carrier of the data used in connection with criminal proceedings (such as magnetic tape containing audio recordings of telephone conversations) remains intact until the end of the trial and that the defence has access to it.

2. In its Interim Resolution DH(2005)57[9] adopted in the *Rotaru* case, the Committee of Ministers took note of a series of developments at national level since the European Court's judgment. The Committee thus noted with interest that Law No. 535/2004 on preventing and combating terrorism had introduced a judicial review procedure prior to any secret surveillance measure in all cases involving threats to national security referred to in Law No. 51/1991.

3. However, the Committee noted with regret that several other shortcomings mentioned by the European Court had not been addressed even though a legislative procedure was then underway to reform the national security laws. These shortcomings concerned in particular the absence of regulations on the age of information that may be retained by the authorities and the impossibility of challenging the retention and truth of that information. The Committee consequently called on the authorities to expedite the legal reforms needed in response to the European Court's criticism of the Romanian system of gathering and archiving information by the intelligence services.

4. Law No. 255/2013 amended both law No. 51/1991 and Law No. 14/1992. These amendments have introduced a number of safeguards to ensure respect for privacy.

II. SCOPE OF SECRET SURVEILLANCE

5. Section 3 of Law No. 51/1991 enumerates the deeds and actions that are regarded as "threats to national security" and may justify the use of secret surveillance measures.[10] Its wording is fairly broad in scope, but following the amendments introduced by Law No. 255/2013 these provisions are currently left to the interpretation of the judge authorising the use of this type of measure (see section III below). This control appears to provide **sufficient safeguards against a broad interpretation of these provisions**.

6. In addition, Law No. 255/2013 gives an exhaustive list of the type of activities that may be carried out by the intelligence services in situations described as "threats to national security". **This responds to the European Court's criticisms in this regard**.

7. On the other hand, the laws governing the SRI's activities still do not determine the categories of persons that may be subjected to such measures, nor do they specify the type of data that may be gathered as a result of these measures. **The authorities should therefore provide indications on the manner in which the envisage clarifying these aspects.**

III. AUTHORISATION FOR ACTIVITIES CARRIED OUT BY THE INTELLIGENCE SERVICES

---

and Others, judgment of 24 May 2011, final on 28 November 2011, § 174.

6 *Bucur and Toma*, cited above, § 164.

7 *Rotaru,* cited above*,* § 72 and *Bucur and Toma,* cited above, §§ 171–173.

8 *Rotaru*, cited above, § 60 and *Dumitru Popescu (No. 2)*, cited above, §§ 74–77.

9 Adopted by the Committee of Ministers on 5 July 2005 at the 933rd meeting (DH) of the Ministers' Deputies

10 See in this connection the information provided by the Romanian authorities and summarised in the appendix to the interim resolution adopted in the Rotaru case.

8. Law No. 255/2013 requires a court authorisation for intelligence-gathering activities that restrict the exercise of fundamental rights and freedoms (referred to below as "specific intelligence-gathering activities"). The authorisation procedure is similar to that introduced by Law No. 535/2004 on preventing and combating terrorism, welcomed at the time by the Committee of Ministers,[11] but includes a number of additional safeguards.

9. Under the new provisions, these activities must be authorised by judges assigned by the President of the High Court of Cassation and Justice to the examination of this type of application. The same procedure must be followed to extend or supplement the initial authorisation.[12]

10. The intelligence service that applies for the authorisation must provide the judge with information on the facts and circumstances that point to the existence of a threat to national security and justify the use of this type of measure. It must also explain to the judge why it is necessary to employ the measure concerned. In his/her assessment, the judge must take account of the fact that under the new provisions he/she may only authorise this type of activity when it is strictly necessary and proportionate to the aim pursued. **These provisions provide important safeguards against the broad and unjustified use of this type of activity**.

11. Exceptions to judicial authorisation are permitted only in emergencies. In these situations, however, the activities must be authorised by the public prosecutor, are limited to 48 hours and are subject to ex post facto review by the judge, who can order the intelligence services to cease their activities immediately and to destroy the data gathered. Law No. 255/2013 provides that the judge shall deliver his/her decision "without delay". If the judge orders the destruction of the data, this must be done within seven days of his/her decision. The new regulations **accordingly provide safeguards that, at first sight, appear capable of ensuring that the authorities will make sparing use of this exception and only do so in duly justified cases.**[13]

12. In conclusion, **the new legal framework governing the authorisation of specific intelligence-gathering activities appears overall to meet the relevant requirements of Article 8**. With regard to the related matter of how domestic law guarantees that the activities in question are actually carried out within the limits of the authorisation, reference is made to the considerations in section VI below.[14]

IV. LIMITS TO THE DURATION OF THE AUTHORISATION FOR SPECIFIC INTELLIGENCE-GATHERING ACTIVITIES

13. Under the old regulations, the initial authorisation, given by the public prosecutor, could be valid for six months. The public prosecutor could extend it for consecutive periods of three months, with no overall limit, an aspect criticised by the European Court.[15]

14. Law No. 255/2013 now provides that the judge's initial authorisation may be given for the duration necessary to complete the surveillance measures but must not exceed six months. It may be extended for valid reasons, but each extension must not exceed three months. The total duration of activities based on the same data indicating the existence of a threat to national security is limited to two years. The activities must end before the (initial or renewed) authorisation expires if there is no longer any justification for continuing them.

15. By imposing an overall limit of two years, the new provisions have **therefore addressed the shortcomings of the old regulations highlighted by the European Court**, especially as Law No.

---

11 See paras. 7–8 of the document, on the interim resolution adopted in the *Rotaru* case.

12 For the total duration of extensions granted, see section IV.

13 See in this connection the judgment in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, 28 June 2007, final on 30 January 2008, § 82.

14 See in this connection the Report on the Democratic oversight of the Security Services (CDL-AD(2007)016, adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007) § 213.

15 *Dumitru Popescu (No. 2),* cited above, § 70.

255/2013 provides that these activities must end before the expiry of this period if the reasons for them cease to exist.

V. PROCESSING OF DATA COLLECTED

1. General questions on the processing of data

16. The European Court repeatedly noted that the law applicable at the material time contained no rules on the processing of data collected through secret surveillance. In particular, Law No. 14/1991 contained no provision on persons authorised to consult information held by the SRI, the nature of that information, the use to which it could be put and the procedure to be followed.[16] Moreover, neither Law No. 51/1991 nor Law No. 14/1992 laid down limits on the age of information held or specified the retention period or the conditions in which intelligence obtained through secret surveillance had to be destroyed.[17]

17. Law No. 255/2013 did not provide any clarification regarding the aforementioned aspects. It is therefore important for the Romanian authorities to specify the law applicable and how it addresses the following questions:

- the procedure to be followed for examining, using and retaining data gathered through secret surveillance activities; and
- the retention period for this type of data as well as the conditions for destroying it and the procedure to be followed.[18]

2. Questions on the use of data in connection with criminal proceedings

18. In the *Dumitru Popescu (No. 2)* case*,* the data collected by means of telephone tapping had been used as incriminating evidence against the applicant in criminal proceedings. In this connection, the European Court held that Law No. 51/1991 contained no provisions to ensure that recordings of telephone conversations remained intact and complete until the end of the proceedings. In the Court's opinion, although it may be permissible for only partial transcriptions of this type of conversation to be placed in the investigation file the accused must nevertheless be offered the possibility of listening to and challenging the truth of the recordings. It is consequently necessary to keep these recordings intact until the end of the criminal trial and, at the request of the defence, to permit transcriptions of other parts of these conversations that may prove useful to it to be placed in the investigation file.[19]

19. In response to these findings, Law No. 255/2013 now provides that data and intelligence collected in the course of specific information-gathering activities shall be transferred to a written medium and sent to the prosecuting authorities when they point to the preparation or commission of a criminal offence. The transcription of the intercepted communications and/or recorded images must be transmitted in full to the aforementioned authorities together with the original digital data carrier. This transmission must be accompanied by a proposal to declassify all or part of the decision to authorise the surveillance activities and the judicial warrant.

20. The new provisions accordingly ensure that in the case of criminal proceedings the prosecuting authorities are in possession of the original carriers of data gathered by the intelligence services. However, they do not provide for the person prosecuted or his/her representative to have access to these data carriers. It is therefore important **to obtain information on the provisions governing**

---

16 *Rotaru,* cited above, § 57.
17 *Bucur and Toma*, cited above, § 164.
18 See the *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* judgment, cited above, § 76. For an example of appropriate legislation, see *Weber and Saravia v. Germany* (application declared inadmissible), 29 June 2006, §§ 45–50).
19 See §§ 78–79 of the judgment.

access by the defence to the original carrier of information gathered through secret surveillance measures justified by national security considerations.

VI. OVERSIGHT OF SPECIFIC INTELLIGENCE-GATHERING ACTIVITIES

21. At the material time, Law No. 51/1991 provided that the activities of the intelligence services must be subject to parliamentary scrutiny. Law No. 14/1992 specified that responsibility for scrutinising the SRI's activities lay with a joint committee of the two chambers of parliament. The organisation and operation of that committee and the arrangements for overseeing those activities were to be established by a decision of parliament. The Court pointed out that, as originally drafted, these Acts did not lay down effective procedures for overseeing information-gathering activities carried out by the intelligence services.[20]

22. The only change made by Law No. 255/2013 in this connection has been a provision incorporated into Law No. 14/1992 according to which specific information-gathering activities carried out by the SRI are also subject to parliamentary scrutiny, within the limits and under the conditions provided for by law. Accordingly, under the present system as long as the person targeted or affected has not been informed about secret surveillance measures carried out in relation to him/her (see sections VII and VIII below), parliamentary scrutiny is the only form of supervision regarding these activities.

23. The European Court has repeatedly emphasised the need to subject these activities, including the processing of data gathered, to the scrutiny of an authority or public official external to the services that carry them out or possessing qualifications such as to guarantee their independence and adherence to the rule of law.[21] This scrutiny is the only safeguard against arbitrariness for individuals targeted or affected by surveillance measures as long as they have not been informed about these activities and cannot pursue the legal remedies provided by domestic law.

24. The Court has considered it desirable in principle for this oversight to be entrusted to a judge.[22] However, non-judicial oversight can, at least initially, be substituted for judicial oversight on condition that the exclusion of the latter does not exceed the limits of what can be regarded as necessary in a democratic society.[23] Whatever the nature of the oversight provided for by law, the existing procedures must provide appropriate safeguards equivalent to those provided by judicial supervision that protects the rights of the individual, and the values of a democratic society must be followed as faithfully as possible in these supervisory procedures.[24] These procedures should enable the authority concerned to check that the activities in question have actually been carried out within the limits laid down by law and by the judge's decision to authorise them, as well as to check that the data gathered have indeed been destroyed in those cases where their destruction is mandatory.[25]

25. In the light of these criteria, it must be concluded that **the framework laid down by Law No. 255/2013 for the parliamentary scrutiny of the intelligence services' activities is unsatisfactory**. This law contains no details on how this scrutiny is carried out. It says nothing about the composition of the body responsible for the scrutiny, the extent of the scrutiny, the qualifications required of those tasked with carrying it out, the body's powers and functions, the procedure to be followed or the measures the body can take if the authorities that have carried out the surveillance are in breach of the law.[26] Nor does this law contain any details on access by the supervisory body to relevant

[20] See § 60 of the *Rotaru* judgment.
[21] See *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 85, and *Rotaru*, cited above, § 60.
[22] See *Klass*, judgment of 6 September 1978, § 55.
[23] *Klass*, cited above, § 56.
[24] *Klass,* cited above, § 55.
[25] Ibid.
[26] Criteria that follow in particular from the *Klass* judgment, cited above, § 56 and the *Dumitru Popescu (No. 2)* judgment, cited above, § 77.

information and expertise, which are essential elements for the supervision to be effective.[27] The *"Association "21 December 1989" and Others v. Romania* and *Bucur and Toma v. Romania* judgments highlight as a matter of fact **the ineffectiveness of the oversight of the intelligence services' activities exercised by the parliament.**

26. The above considerations show **the importance for the authorities to review the current mechanism of oversight of the intelligence services' activities, especially those that interfere with the exercise of rights and fundamental freedoms**, in order to determine the measures required to ensure its independence and effectiveness. The authorities could well draw inspiration in this connection from the many Council of Europe documents on this subject.[28]

VII. INFORMING PERSONS WHOSE RIGHTS AND FREEDOMS HAVE BEEN INFRINGED IN THE COURSE OF SPECIFIC INTELLIGENCE-GATHERING ACTIVITIES

27. As originally drafted, Laws Nos. 51/1991 and 14/1992 did not provide for the obligation for the authorities to inform the persons concerned about the secret surveillance activities to which they had been subjected or which had affected them.

28. Law No. 255/2013 now obliges the head of the intelligence service to inform persons concerned about activities relating to them when the data and intelligence obtained (i) do not allow the case to be referred to the prosecuting authorities and (ii) do not justify continuing the intelligence-gathering activities in respect of those persons. **This change marks an important step forward compared with the former system**.

29. This Law also provides for exceptions to providing information. Thus, even if the aforementioned conditions are met the persons concerned will not be informed when the information could compromise the operations of the intelligence services, have an impact on the defence of national security, adversely affect the rights and freedoms of others or reveal the methods and investigation techniques employed by the services responsible for national security.

30. However, if it can be acceptable to delay the provision of information for the reasons mentioned in the previous paragraph,[29] the lack of information can no longer be justified once those reasons no longer exist. It therefore appears **necessary to provide in the law for the intelligence services to be obliged to inform the person concerned about the activities that have targeted or affected him/her as soon as the reasons that stand in the way of providing that information have ceased to exist.**[30]

31. In addition, since access to the legal remedies provided by law (see section VIII below) depends, in most cases, on that information, **the decision of the head of the intelligence service to delay providing the information should be subjected to the scrutiny of an independent and impartial authority**. That scrutiny should in particular make it possible to balance the interests that justify delaying passing on the information against the competing interest of the person concerned in knowing that he/she has been targeted or affected by secret surveillance activities in order, if

---

[27] See Resolution 2045 (2015) of the Parliamentary Assembly of the Council of Europe on mass surveillance.

[28] See in this connection the aforementioned Resolution 2045 (2015) of the Parliamentary Assembly of the Council of Europe and the issue paper "Democratic and effective oversight of national security services" (2015) published by the Council of Europe Commissioner for Human Rights (CommDH/IssuePaper(2015)2, 5 June 2015). See also the above-mentioned Venice Commission Report on Democratic Oversight of the Security Services and the update of the 2007 Report on Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015).

[29] See, inter alia, *Klass*, § 58.

[30] On this point, see *Weber and Saravia* (application declared inadmissible), cited above, § 135, and the case law referred to there.

necessary, to make use of the legal remedies available under domestic law. The comments in section VI above thus also appear relevant in this context,

VIII. LEGAL REMEDIES

32. The European Court pointed out that at the relevant time no legal provision enabled the intelligence services' retention of data on an individual's private life to be challenged or the truth of that information to be refuted. [31]

33. Law No. 255/2013 now provides that everyone who considers his/her fundamental rights or freedoms to have been infringed owing to specific intelligence-gathering activities can refer the matter to parliamentary committees charged with supervising those activities. According to this Act, these individuals can also take legal action on the basis of the relevant provisions of the Civil Code, the Code of Criminal Procedure or the Protection of Personal Data Act[32].

34. With regard to *all these remedies,* it should be noted that the legality and procedural regularity of specific intelligence-gathering activities can only be verified if the review body has access to the decision and to the judicial warrant authorising those activities. The authorities should therefore **indicate the conditions and procedure for ensuring access to this type of documents by national bodies once they have had a case referred to them under one of these remedies**

35. With regard to the possibility of referring a case to a *relevant parliamentary committee*, the European Court has stated that " the mere possibility – provided for by section 16 *in fine* of Law No. 51/1991 – for an individual to refer to the committees […] of the two chambers of the national parliament cannot compensate for the absence of any prior or ex post facto supervision of phone tapping by an independent and impartial judicial authority […] since the law did not provide for any sanction or measure that the parliamentary committees would have had the power to impose in the event that the authorities which carried out or authorised the intercepts were in breach of the law".[33] Since Law No. 255/2013 says nothing more on the extent of the powers of these committees, the European Court's findings remain valid, and **this avenue accordingly does not appear to be able to constitute an "effective remedy" within the meaning of Article 13 of the Convention**.

36. As far as the possibility of referring a matter to the *courts* is concerned, more information is needed to assess whether the remedies mentioned in Law No. 255/2013 meet the requirements of an effective remedy. The main questions that arise in this connection are as follows:

(i) with regard to bringing a civil action: information is necessary on the provisions of the Civil Code under which an action for damages can be brought and enable the courts (i) to order the immediate cessation of all activities interfering with the rights guaranteed by the Convention, when the interference stems from the activities of the state authorities, including the intelligence services, and (ii) to decide what is to be done with the intelligence gathered as a result of those activities.

(ii) with regard to an action based on the Protection of Personal Data Act: this Act does not apply to "the processing and transfer of personal data carried out in connection with activities linked to defence and national security, which were carried out in compliance with the limits and restrictions provided for by law" (section 2.7). In point of fact, activities carried out by the intelligence services pursuant to Law No. 51/1991 are by definition linked to national security. In these circumstances, the authorities should state how the restriction under section 2.7 can be reconciled with the possibility of bringing an action based on this Act before the courts when a person considers himself/herself wronged by the activities of the intelligence services.

---

31 See, for example *Rotaru*, cited above, § 72 and *Bucur et Toma*, cited above, § 171.

32 Act no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

33 *Dumitru Popescu (No. 2)*, cited above, § 77.