Strasbourg, 22 October 2018 **CDL-AD(2018)024**

Opinion No. 936 / 2018 Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

REPUBLIC OF MOLDOVA

OPINION

ON THE LAW

ON PREVENTING AND COMBATING TERRORISM

Adopted by the Venice Commission
at its 116th Plenary Session
(Venice, 19-20 October 2018)

on the basis of comments by

Ms Claire BAZY MALAURIE (Member, France)
Mr Iain CAMERON (Member, Sweden)
Mr Dan MERIDOR (Member, Israel)
Ms Grainne McMORROW (Substitute Member, Ireland)

Table of Contents

I. Introduction

1. By letter of 2 August 2018, Ms Victoria Iftodi, the Minister of Justice of the Republic of Moldova, requested an opinion from the Venice Commission on the Law on Preventing and Combatting Terrorism (CDL-REF(2018)046), hereinafter referred to as Law no. 120 or the Law.

2. Ms Claire Bazy Malaurie (Member, France), Mr Iain Cameron (Member, Sweden), Mr Dan Meridor (Member, Israel), and Ms Grainne McMorrow (Substitute Member, Ireland), acted as rapporteurs for this opinion. On 20-21 September 2018, a delegation composed of Ms Bazy Malaurie, Mr Meridor, and Ms McMorrow, accompanied by Mr Grigory Dikov, legal officer at the Secretariat, visited the Republic of Moldova, and met with the representatives of the State authorities, politicians, NGOs and other stakeholders. The Venice Commission is grateful to the Moldovan authorities for the preparation of the visit.

3. The English translation of Law no. 120 was provided by the authorities of the Republic of Moldova. Inaccuracies may occur in this opinion as a result of incorrect translation.

4. The present opinion was prepared on the basis of the contributions of the rapporteurs, and adopted by the Venice Commission at its 116th Plenary Session (Venice, 19 - 20 October 2018).

II. Analysis

A. Scope of the opinion

5. The request by the Ministry of Justice was prompted by the recommendation of 4 August 2017 by the EU – Republic of Moldova Association Council. The Council had suggested assessing Law no. 120 with regard to its compliance with human rights standards (see p. 2.3 of the Recommendation). Consequently, Law no. 120 will be assessed from the human rights' perspective.

6. The primary concern of this opinion is not casting aspersions on the work and practices of the Secret Intelligence Service (the SIS),[1] i.e. the body responsible under Law no. 120 for preventing and combating terrorism, but with assisting the Republic of Moldova in getting the operational framework right.

7. This opinion does not cover all issues which may arise in relation to Law no. 120. This Law has been in operation only since September 2017, and since the Republic of Moldova has been fortunate in not being a target for terrorists, there is little or no jurisprudence or administrative practice in this area. Consequently, the Venice Commission will focus on those elements of the Law which may potentially lead to abuses, even if the application of this Law has not, to date, or at least as yet to the best of its knowledge, given rise to major issues.

8. This opinion does not address the questions of the infrastructure (by regulation or otherwise) necessary to deal with the practical realities following incidence of terrorism. Such infrastructure may consist of provision for special detention centres, specialised courts, and protective measures governing the involvement of citizens in the apprehension of suspected terrorists, and accompanying safeguards, training programs for the security services personnel, etc. However, the practical importance of such infrastructure should not be underestimated.

B. A short outline of Law no. 120

9. Law no. 120 describes the role and the powers of the SIS in the field of the fight against terrorism, as well as the corresponding obligations of the public bodies and private actors in this area.

[1] This is the name of the Service contained in the current English translation of the Law.

10. Chapter I gives a definition of "terrorism", "terrorist activity" and of other terms used by the Law, and sets out the general principles of the public policy in this area. Chapter II describes the institutional framework of anti-terrorist activities, with the SIS in the centre of it, and other State authorities playing a subordinate role in their respective fields.

11. Chapters III and IV deal with two main tasks of the SIS: (a) prevention of terrorism, and (b) combating terrorism. "Prevention" (described in Chapter III) involves assessing risks related to the terrorist activities, identifying legal entities and persons involved in the terrorist activity, and enhancing protection of objects of "critical infrastructure". "Prevention" is a routine work, exercised permanently and on all national territory. "Combating" terrorism (described in Chapter IV), by contrast, means responding to a terrorist crisis when it is happening or about to happen (an attack, a hostage taking, etc.), where there is an "imminent threat" to the vital public interests. The legal regime of "combating terrorism" is exceptional: it is triggered by a decision of a competent body, covers a particular geographical zone, and, by all appearances, at least, is of a limited duration.

12. Finally, the Law establishes liability for terrorist propaganda in the mass-media and, more broadly, on the Internet, provides for the liquidation of private entities affiliated with the terrorists, and fixes rules on the compensation of damage caused by the terrorist activities (Chapters V-VIII).

C. Definition of "terrorism", "terrorist activity" and other terms used in the Law

13. Law no. 120 explains, in Article 3, what is meant by "terrorism" (and its derivatives, like "terrorist activity", "terrorist crisis" etc.). The Venice Commission is aware of the absence of an internationally agreed and comprehensive definition of terrorism, and of the difficulty related to giving a clear definition to it in the national legislation.[2] However, definitions contained in the Law are overly broad and all-encompassing.

14. Thus, to give a definition of "terrorist activity", the Law refers to "terrorist acts" and "terrorist offences", as punishable under the Criminal Code, and, in addition, formulates its own lengthy definition of the "terrorist activity" which the SIS is supposed to fight.[3] This may mean that the SIS and other State authorities mentioned in the Law are dealing with something which is not criminal in nature. One may conclude that this is a *sui generis* activity, governed by different rules.

15. The definition of a "terrorist act" given by the Criminal Code is by itself too broad. For example, to be categorized as a "terrorist act" it suffices that it represents a "threat of committing" of "an act that creates the danger of […] substantial damage to property or the environment […] in order to draw the public attention to certain political […] views of the person who committed the act". This may include a threat to hold a labour union strike which may (probably) cause damage

[2] See Basic Human Rights Reference Guide: Conformity of National Counter-Terrorism Legislation with International Human Rights Law, 2014, OHCHR, p. 24.

[3] Full quote: "terrorist activity (terrorist activities) – activities, comprising:
– planning, preparing, the attempt to commit and committing a terrorist act or any other act, which constitutes a terrorist offence;
– the formation of an illegal armed group, of a criminal organization, of an organized group for committing one or more terrorist offences;
– recruitment, favouring, arming, training and use of terrorists;
– adherence to terrorist organizations or participation in the work of such organizations;
– financing the training or committing of a terrorist act or any other terrorist offence, financing a terrorist organization, of a terrorist group or a terrorist, as well as providing them with support by other means;
– the provision of information support or of any other type in the process of planning, preparing or committing of a terrorist act or of any other act constituting a terrorist offence;
– instigation for terrorist purposes, public justification of terrorism, the propaganda of the ideas of terrorism, distribution of materials or information aimed at terrorist activities or entitling to carrying out such activities;
– any of the aforementioned actions performed via information systems and electronic communication networks;
– any other acts constituting a terrorist offence."

to the property interests, or a large and boisterous demonstration. These acts may not be polite. They may even be illegal, but they are definitely not "terrorist acts". It may be legitimate and necessary to cope with them, but not with all the exceptional powers given to the State in case of terror. In sum, it is necessary that both the Criminal Code and Law no. 120 give a definition of terrorism (and its derivatives) which is as narrowly formulated as possible, and mutually consistent. International perspectives on how best to protect human rights alongside laws introduced to prevent and combat terrorism strongly favour their being aligned, whenever possible, within the framework parameters and jurisprudence of the criminal law.

16. A very broad definition of "terrorist activity" in the Law raises another question, namely whether the law is intended to cover the situation in Transnistria – a part of the territory of the Republic of Moldova *de facto* controlled by a separatist government. On the one hand, nothing the rapporteurs heard suggested that the purpose of the Law is directed towards resolving this particular political issue. On the other hand, however, the situation in Transnistria may be arguably characterised as, for example, "creation of an illegal armed group", which is a terrorist activity according to Article 3 of the Law. So the question arises as to whether the special powers received by the SIS to prevent and, in particular, to combat terrorism may also be used against the separatists. If this is so, it could mean that the whole Transnistria region may be designated as a separate zone where the SIS has special competencies provided by the Law, and this on a quasi-permanent basis. It is unclear whether this is the intention of the legislator. While it is legitimate to devise special legal tools to tackle the problem of separatism, it is highly questionable as to whether the extraordinary legal mechanisms developed for the fight against terrorism are appropriate in the context of separatism. The Venice Commission invites the Moldovan authorities to consider this question.

D. Relation between Law no. 120 and other applicable legislation

17. The Moldovan legislation related to the activities of the SIS is very fragmented, partly overlapping and unhelpfully lacks clarity regarding its chain of command and operational process. The Venice Commission has previously examined several laws or bills in this area which concerned the investigative powers of the SIS,[4] fight against cybercrime,[5] the status of the SIS itself,[6] and State secrets.[7] In the 2006 opinion the Venice Commission expressed the regret that "the exact significance of many provisions [of the law on the SIS] can be difficult, if not impossible to grasp on account of the many general references to other legislation, often without further precisions".[8] A similar remark is called for in the context of Law no. 120.

18. Besides the fight against terrorism, the SIS performs other tasks (such as, for example, combating corruption, cybercrime, etc.)[9] which are regulated by other laws. In addition to those "sectorial" laws, the powers of the SIS and the procedures it follows are described in:

- the law on the SIS (Law no. 753),
- the law on the special investigative activities (Law no. 59),
- the Criminal Procedure Code (the CPC),
- the Administrative Code,

[4] CDL-AD(2017)009, Republic of Moldova - Joint Opinion of the Venice Commission, the Directorate of information society and action against crime and of the Directorate of Human Rights (DHR) of the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the Draft Law no. 281 amending and completing Moldovan Legislation on the so-called "Mandate of security"; see also CDL-AD(2014)009, Joint Opinion of the Venice Commission and the Directorate General of Human Rights (DHR) and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the draft law on amending and supplementing certain legislative acts, promoted by the intelligence and security service of the Republic of Moldova.

[5] CDL-AD(2016)039, Republic of Moldova - Joint Opinion of the Venice Commission and of the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the Draft Law N°161 amending and completing Moldovan Legislation in the field of Cybercrime

[6] CDL-AD(2006)011, Opinion on the Law on the information and security service of the Republic of Moldova

[7] CDL-AD(2008)008, Opinion on the Law on State Secret of the Republic of Moldova

[8] CDL-AD(2006)011, § 9

[9] See Article 7 of the Law on the SIS (in Romanian or Russian): http://lex.justice.md/ru/311721/

- the law on personal data protection (Law no. 133), etc.

19. This fragmentation creates uncertainty as to what checks and limitations exist on the SIS's powers. Law no. 120 confers on the SIS some new powers related to information gathering, to be used for the prevention of the terrorist activity and in counter-terrorist operations. The question arises whether this Law creates a *new* legal regime, exempted from the general rules provided by the CPC and Law no. 59.

20. The power to conduct criminal investigations in the Republic of Moldova belongs *exclusively* to the General Prosecutor's Office (GPO).[10] While the SIS cannot conduct criminal investigations on its own, it may take "special investigative measures" under Law no. 59 (see Article 6 (1) of the Law on the special investigative activities[11] and Article 10 (1) (a) of the Law on the SIS).[12] Thus, Law no. 59 seems to be relevant to the information gathering activities conducted by the SIS. The question, however, remains: does Law no. 59 govern *all* aspects of the SIS's information gathering work, and in particular to the tasks performed under Law no. 120?

21. The Venice Commission recalls that in two opinions of 2014 and 2017 it examined draft legislation introducing a so-called "security mandate" – a parallel system of surveillance *outside* of a criminal investigation context. The need to introduce the "security mandate" was explained by the fact that the mandate of the SIS was broader than just investigation *into specific crimes*, and that ordinary procedures provided by the law on the SIS (Law no. 753), and by the law on the special investigative activities (Law no. 59), were not adapted to it. Those draft amendments have not been enacted; however, the very idea of a "security mandate" shows that some of the activities of the SIS go beyond the pure criminal-law context, and escape the ordinary rules set out in Law no. 59.

22. In principle, security services may pursue a range of goals, not necessarily limited to the prosecution of specific crimes. As the Venice Commission noted in the 2014 opinion, "activity potentially damaging to the security of the state may not have reached the threshold of a criminal offence, even a preparatory or other inchoate offence".[13] This is also true in respect of the fight against terrorism and prevention of terrorism – besides surveillance targeted on particular suspects, the intelligence service may be involved in the strategic surveillance and other forms of gathering of information.[14]

23. Law no. 120 however does not explain which powers of the SIS are governed by the ordinary legislation, and which are governed by the special rules, and what those rules are. During the visit to Chisinau the authorities assured the rapporteurs that general limitations and checks on the SIS' powers are *fully* applicable in the context of Law no. 120, where "special investigative measures" are concerned. This is probably so, but in the absence of settled jurisprudence and clear legislative context it is difficult to confirm this assertion. In any event, Law no. 120 is silent on this point, and only rarely refers to other *specific* pieces of legislation.[15]

24. The Venice Commission cannot assess all the legislation relevant to the SIS and its activities. The present opinion is focused primarily on Law no. 120. In future, however, it would be very useful to evaluate the legislation related to the SIS *as a whole*. The positive assertion the rapporteurs heard from the Moldovan side during the visit, regarding the validity and applicability of all human rights guarantees prescribed in the CPC and Law no. 59 to the powers listed in Law

[10] Law no. 120 stipulates, in Article 7 (2), that it is a duty of the General Prosecutor's Office [(the GPO)] to "carry out the activity on preventing and combating terrorism by conducting and exercising the criminal prosecution in respect thereof".
[11] See (in Romanian or Russian) http://lex.justice.md/index.php?action=view&view=doc&lang=2&id=343452
[12] See (in Romanian or Russian): http://lex.justice.md/index.php?action=view&view=doc&lang=2&id=311721
[13] CDL-AD(2014)009, § 24
[14] See CDL-AD(2015)011, Report on the Democratic Oversight of Signals Intelligence Agencies, § 47
[15] Besides some general references to law in general

no. 120 should be clearly written in Law no. 120. In addition, regulations intended to govern the application of Law no. 120 which are currently being drafted within the SIS could usefully include reference to all applicable legislation pertinent to the SIS.

E. Institutional framework of the fight against terrorism

25. Under Article 6 (2), the Government "is the main authority responsible for the organisation of the activity on preventing and combating terrorism". The SIS, however, is the body which "*directly* carries out the activity on preventing and combating terrorism" (Article 6 (3), emphasis added). It does so by gathering information, developing general rules and policies, and, in times of a crisis, by intervening *manu militari*.

26. Other authorities (the GPO, the Ministry of Interior, the Ministry of Defence, the Ministry of Economy and Infrastructure, the Ministry of Health, Labour and Social Protection, etc.) are involved in the anti-terrorist activities in their respective fields: for example, the Customs Service has to prevent the smuggling of weapons and explosives, which may be used to commit terrorist crimes.

27. In addition, under the Law the Speaker of Parliament has certain powers in this field: she/he "coordinates the entire activity of the preventing and combating terrorism" (Article 6 (1)), and, in the case of a terrorist crisis, the Speaker, together with the Director of the SIS, orders the creation of the Counter-Terrorist Command (the CTC), and appoints the head of the CTC (see Article 25 (2)).

28. It is very unusual to give the Speaker – a representative of the legislative body – the function of coordination of activities of several executive bodies; in addition, one may have doubts whether this would result into a mere "rubber stamping" exercise. In the opinion of the Venice Commission, it would be more appropriate to entrust the Government as a whole (or a specific ministry, service or agency within it) with this function. This recommendation does not exclude that Parliament should keep control over the SIS,[16] in particular through the Committee on Security.[17] However, the parliamentary control exercised *ex post* should not be assimilated with the routine coordination which is an "executive" activity and for which the Government should be responsible, politically and otherwise. It is not clear whether the Speaker and the Government are in a hierarchical relationship (given that the Government is identified as "main authority" responsible for anti-terrorist activities, and the Speaker has the task of "coordinating the entire activity" in this field).

29. As concerns parliamentary control, according to Article 20 of Law no. 753 (Law on the SIS), the SIS is required to report on its activities to Parliament, once a year. In addition, the Committee on Security exercises control over the activities of the SIS through a relevant sub-committee. However, Law no. 753 and Law no. 120 do not specify what form this control may take. As it was explained during the meetings in Parliament, in practice the sub-committee never goes beyond a mere discussion of a general report prepared by the SIS. The sub-committee never looks into the specific files, nor questions the staff of the SIS, etc. This is worrying: while it is inappropriate to give the Speaker nominally the power to coordinate anti-terrorist activities, it is absolutely necessary to strengthen the parliamentary control by specifying which investigative powers the sub-committee has vis-à-vis the SIS.[18]

---

[16] In 2016 the SIS was transferred under the jurisdiction of Parliament (see CDL-AD(2017)009, § 14) – that may explain why the Speaker is designated as a "coordinating authority" under Law no. 120.

[17] See Article 20 (only in Russian or in Romanian languages): http://lex.justice.md/index.php?action=view&view=doc&lang=2&id=311721

[18] In CDL-AD(2017)009 the Venice Commission stressed that "some mechanism of continuous independent oversight is also necessary" (§ 33). The ECtHR, when discussing the parliamentary control over secret surveillance operations noted as follows: "The Court is not persuaded that this scrutiny [by a Parliamentary committee] is able to provide redress to any individual grievances caused by secret surveillance or to control effectively, that is, in a manner with a bearing on the operations themselves, the daily functioning of the surveillance organs, *especially since it does not appear that the committee has access in detail to relevant*

30. In the 2017 opinion on the "security mandate" the Venice Commission made the following proposal: to establish a security-screened expert body, possibly with political representation on it, and/or with respected members of civil society, with the competence of oversight of the SIS activities.[19] It appears that, despite this recommendation, such a follow-up expert monitoring body has not been created. Whereas such a body will not be a cure-all solution against possible abuses of or by the SIS, it may be instrumental in reducing the risk of such abuses, so the Moldovan authorities are invited to give this option a serious consideration.[20] In both cases (the existing sub-commission or the mixed expert body) it is necessary to ensure a strong presence of the representatives of the opposition on this body.

31. Finally, any *ex post* control by a parliamentary sub-committee (or a mixed expert body) would be wholly inefficient if there are no rules requiring record-keeping within the SIS, and if there are no "paper trails" of actions (especially those related to the surveillance) taken by the SIS.[21] During the visit to Chisinau the rapporteurs were told that internal regulations are now being developed within the SIS. It is crucial that those regulations put in place a record-keeping system. The law must also provide for access by the parliamentary sub-commission (or the mixed expert body) to those records, and the records should correspond to certain parameters (they should outline the reasons for specific actions of the SIS, their duration, extent, the information obtained, etc.).

F. Powers of the SIS

32. As noted above, Law no. 120 distinguishes between ordinary powers of the SIS (mostly to be used in the context of "prevention" of terrorism) and extraordinary ones (which are to be used only during a terrorist crisis). The Venice Commission will examine the ordinary powers of the SIS first.

33. Before addressing this issue, the Venice Commission acknowledges that "a State needs effective intelligence and security services: intelligence is thus an inescapable necessity for modern governments". "Security services […] by their very nature, impinge on individual rights. It is therefore essential that there be internal limits as well as external limits to their activities".[22] The question is where the Law puts those limits. Laws which provide for responses to extreme, unpredictable, and volatile circumstances inevitably compromise citizens' rights and freedoms enjoyed in normal circumstances; which is why these laws need to meet established human rights standards and strike the difficult balance of not obstructing the ability of the State to counter terrorism, whilst not facilitating the introduction of an oppressive regime with the unintended risk of that becoming a norm.

1. Powers related to the "prevention" mandate

34. The law entitles the SIS (directly or through a specially created unit – the Anti-terrorism Center – to take, amongst others, the following measures:

- to "define and implement both legislative and normative instruments" related to the anti-terrorist activities (Article 7 (1) (a));
- to issue "compulsory prescriptions" to other state authorities and to private persons (see Article 8 (3));

---

documents. The scope of their supervision is therefore limited […]." (emphasis added; *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016, § 82.

[19] CDL-AD(2017)009, § 34

[20] The Venice Commission is mindful that effective parliamentary control does not give the victims of the surveillance the possibility of obtaining redress (as stressed by the ECtHR in *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016, §§ 36 et seq.), so it should be coupled with the mechanism of judicial review of individual complaints by the victims of surveillance and other persons affected by the activities of the SIS.

[21] CDL-AD(2015)010, Report on the Democratic Oversight of the Security Services (updated), § 153

[22] Ibid, §§ 1 and 2

- to "collect and to process the data" (Article 8 (3) (c));
- to use "all the forces" to identify terrorist activities (Article 16 (1));
- to "[discontinue] the activity of legal persons preventing the proper conduct of anti-terrorist measures" (Article 9 (1) (e));
- to "attract, free of charge, forces and resources [..] of legal persons" (Article 17 (3));
- to issue "anti-terrorist passports"(Article 19);
- to monitor the application of the anti-terrorist measures (Article 20), i.e. to conduct verification visits, which may be unannounced and repeated.

35. In addition, the law formulates corresponding legal duties and responsibilities of private persons:

- the obligation to "provide assistance" and "put at the disposal" of the authorities "movable and immovable property, other objects and documents and the information held by them" (Article 16 (2));
- the duty to participate in the anti-terrorist exercises (Article 17 (2));
- the duty "to ensure access to sites of 'critical infrastructure'", according to the list of such infrastructure composed by the security service itself (Article 10 (g));
- The duty of citizens to "make available…information which can contribute to the prevention of terrorism" (Article 13 (2)).

36. These powers and corresponding duties are dispersed in the text of the Law. The legislator avoided using the language characteristic for criminal investigations ("forced entry into premises", "seizure of documents", "requisitioning of property", "secret surveillance", etc.), but certain provisions of the Law may be construed as giving the SIS coercive powers of a similar nature. These measures may interfere with the privacy of private persons (guaranteed by Article 8 of the European Convention on Human Rights, the ECHR), with their property (guaranteed by Protocol no. 1 to the ECHR), or with both.[23]

37. From the human rights' perspective, any such interference should be *lawful* and *proportionate*. As regards lawfulness, the Venice Commission regrets to note that many provisions of Law no. 120 are so vague that they can hardly be seen as a lawful ground for any interference.[24] For instance, Article 17 (3) permits the SIS, during an "anti-terrorist exercise"[25] to "attract, free of charge, forces and resources [..] of legal persons". Does it mean that the SIS may, for example, occupy premises of a TV-station and thus disrupt its activities, referring to the need to verify whether the building of the station is "terrorist-proof"?

38. Another example is the information gathering by the SIS: Article 8 (3) (c) entitles the SIS to "collect and to process the data", whereas Article 16 (2) obliges private persons to give to the SIS "documents and the information held by them". The law does not specify what sort of information can be requested, and in what circumstances. For example, should a bank, under those provisions, be compelled to give access to the financial information of a client at the first request by the SIS? Should the SIS meet the basic requirement of providing a reasonable explanation as to why it needs certain information, and follow a process of examination of its substantive reasons by a court (or other external body), to obtain an order validating the request?

39. Arguably, the most dangerously broad power of the SIS is the one to "define and implement both legislative and normative instruments" (Article 7 (1) (a)) and issue "compulsory prescriptions" (Article 8 (3)). The law does not explain what those "normative instruments" or "prescriptions" are, and they may therefore be misconstrued as conferring on the SIS a blanket mandate to legislate

[23] The Venice Commission will not comment on gathering of information by the SIS by non-coercive means: from open sources, from the informers or from other State authorities. The same concerns the use by the SIS of the State-owned property and premises. The focus of this Section is on the coercive powers of the SIS vis-à-vis private persons.

[24] The comments below concern coercive powers of the security agency

[25] I.e. a simulation of a terrorist crisis in order to verify whether the authorities and private entities and persons are ready for a terrorist attack

in the area of the fight against terrorism. In sum, this general entitlement of the SIS to "collect data" and the obligation of private individuals and entities to provide "documents and information" is too broadly formulated to be *lawful*, within the meaning of the ECHR.[26]

40. Insofar as the *proportionality* of the measures described above is concerned, it also raises questions. Proportionality may be ensured in many ways. First, the Law itself could define the material circumstances in which the SIS may request and use the information and documents, access private premises, issue "compulsory prescriptions" or take other coercive measures. Law no. 120 however does not do so. It does not mention what particular type of investigation may trigger a request for information; what sort of information may be requested and from whom. It does not set a threshold requirement for the use of those powers,[27] the list of possible targets, etc. This situation is partially due to the very general definition of the "terrorist activity" and of the mandate of the SIS in this sphere, which includes virtually everything which is at least distantly related to terrorism.

41. Secondly, proportionality may be ensured by introducing controls by external independent bodies, verifying that the powers are not abused. However, as transpires from Law no. 120, currently the SIS may exercise those powers almost unchecked. Thus, for example, the authorities responsible for the objects of critical infrastructure (which may be in private ownership – see the definition in Article 3) should ensure access to those objects by the SIS officers. The list of the objects of critical infrastructure is defined by the SIS itself (Article 19 (2)), without any external supervision, and the SIS may conduct unannounced checks of such objects, as often as defined by the SIS (see Article 20 (2), (3) and (4)). It means that the SIS will be able to access certain private business premises, which it identifies as "critical", at any time and without a court warrant.

42. The above does not mean that a court warrant should be required in *all* cases where there is an interference with privacy or property rights. The nature of the procedural safeguard should depend on the nature and seriousness of the interference with the protected right.[28] Thus, it is possible for the law to pre-define certain very specific industrial objects which should be accessible for the SIS without additional authorizations (airports, nuclear power plants, etc.). It is also conceivable that the SIS may obtain certain types of personal data without a court warrant – either automatically (like the information about air passengers, as described in Article 21),[29] or, for example, following a simple notification to a public prosecutor (and, in the most urgent situations, with *ex-post* notification).

43. A model for such regulations is proposed by Article 18 of Law no. 59 (on special investigative activities). It makes a distinction between more intrusive methods of information-gathering, which should be authorised by a court within a criminal case, and less intrusive methods, which are possible on the basis of the decision of a prosecutor.[30] However, as noted below, the applicability

[26] In the case of *Roman Zakharov v. Russia*, [GC], no. 47143/06, ECHR 2015, § 229, the ECtHR held that "the domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures".

[27] Akin the existence of a "reasonable suspicion" against a particular person, which is required to trigger certain investigative measures in the context of criminal proceedings. Concerning the threshold requirement, see, in particular, the case of *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016, §§ 66 et seq.,

[28] CDL-AD(2014)009, Joint Opinion of the Venice Commission and the Directorate General of Human Rights (DHR) and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the draft law on amending and supplementing certain legislative acts, promoted by the intelligence and security service of the Republic of Moldova, § 30: "The European standard is to provide for a graded scale of response: the more the special investigative measure is capable of infringing human rights, the tighter should be the controls on its use". For a very detailed analysis of the police investigative powers in Poland see CDL-AD(2016)012, Poland - Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts

[29] The Venice Commission does not necessarily approve the amount and the character of the information which the air companies are obliged to produce to the SIS; this question has not been thoroughly discussed. However, at least, Article 21 is quite precise as to what information the SIS may collect from the air companies.

[30] This does not mean that the existence of a court warrant is a panacea and excludes abuses. See the case of *Iordachi and Others v. Moldova*, no. 25198/02, 14 September 2009, in which the Court found that "…the system of

of Law no. 59 in the context of Law no. 120 is unclear. Furthermore, certain powers of the SIS (like the power to issue "compulsory prescriptions" or to "attract, free of charge, forces and resources [...] of legal persons") go beyond the purely information-gathering powers described in Law no. 59.

44. In sum, the mandate and the powers of the SIS, insofar as the "prevention" of terrorism is concerned, are formulated in the Law in overly broad terms. The material scope of these powers is not defined, and the Law is silent about external checks which may limit the discretion of the SIS. It is possible that the SIS, in exercising those powers, is limited by other legislation (namely the CPC and Law no. 59), but references to such other laws are not specific and clear enough. Thus, there is a risk that these provisions may be abused.

45. As the matter stands now, this risk of abuses remains theoretical. At least, during the visit to Chisinau the rapporteurs did not hear about any serious allegations of abuses by the SIS. Nevertheless, the Venice Commission recommends that all coercive powers of the SIS under the Law undergo a thorough review, and that in each case the Law should indicate specifically (either by referring to other applicable laws or by formulating it in Law no. 120 directly) the material conditions for using those powers and/or the procedural safeguards associated with the exercise of those powers.

2. Powers related to the "combating" mandate

46. In a situation of a terrorist attack, the SIS forms a Counter-Terrorism Command (the CTC), the body responsible for managing the crisis, and composed of representatives of the SIS and other authorities. The decision to form the CTC is taken by the Speaker, on the proposal of the Director of the SIS. The CTC receives the quasi-plenitude of powers within the zone of the terrorist crisis, which is defined by the head of the CTC (see Article 25 of Law no. 120).

47. The start of an anti-terrorist operation activates a special legal regime, described in Article 27. Once declared, this legal regime is to be publicised via the mass-media. It may involve restrictions on the freedom of movement, the forced evacuation of the zone of the counter-terrorist operation, the suspension of activities of certain industrial sites, a ban on public gatherings, the prohibition of sale of certain dangerous goods and alcohol, etc.

48. Specially authorised officers of the CTC during this period have the power to stop, question and detain people for the purposes of identification, or for the breach of the special regime, to enter homes and private premises, to use transport and communication means belonging to private persons, to intercept telephone calls and other electronic communications, etc.

49. In sum, Article 27 gives the CTC significant emergency powers within the zone, with all other authorities (including police, prosecution, and military) subordinated to the CTC. These extraordinary powers may be justified in the times of a serious terrorist crisis, when normal legal procedures cannot be employed. Several questions, however, remain.

50. First, it appears that the declaration of the legal regime of an anti-terrorist operation needs to be agreed between two officials: the Speaker of Parliament and the Director of the SIS. One can query whether it would not be more appropriate for the relevant government Minister to take the decision to initiate an anti-terrorist operation rather than an official, moreover, an official of the very government agency which will obtain wide-ranging powers during the duration of the anti-terrorist operation. The advantage of giving such a function to a Minister is that there is, first, no question about who has the power to terminate the anti-terrorist operation, as it will be the Minister, and second, that the Minister would act under responsibility to Parliament. Admittedly,

---

secret surveillance in Moldova is, to say the least, overused, which may in part be due to the inadequacy of the safeguards contained in the law". Moreover, the list of "special investigative measures" in Law no. 59 which do not require a court warrant is also open to criticism – but this law is not in the focus of the present opinion.

the need for an anti-terrorist operation might arise suddenly. Nonetheless it should still be possible to contact the Minister and obtain, if need be, oral permission to initiate the operation. One could even give the head of the SIS an interim power to initiate an anti-terrorist operation in cases where any delay, even the short delay involved in contacting the Minister, might cause major risks to life or property. However, the need to use such an interim power would – presumably – be exceptional.

51. As regards the idea of counter-signing the decision to initiate an anti-terrorist operation, the Venice Commission has already noted that it is quite unusual to entrust what is, in fact, an executive power to the Speaker. At the same time, the idea that the decision of the Director of the SIS to launch an anti-terrorist operation needs a counter-signature by another top-ranking official, or an external collegial body, is worth praise. As explained below, the regime of an anti-terrorist operation is akin a mini "state of emergency", so it needs a proper external approval to avoid abuses.

52. The Venice Commission noted, in respect of the "state of emergency" regime, that "despite the common conviction that the imposition of a state of emergency is always 'time for executive power', contemporary constitutionalism provides for regulations to guarantee the role of Parliament in this process".[31] The Venice Commission recalls that under Article 15 of the ECHR derogation from rights is permissible in cases of "war or other public emergency threatening the life of the nation". Whether there exists a public emergency or not is ultimately a matter for the ECtHR, even if a large margin of appreciation is granted to the State in such context.

53. The Venice Commission has been informed that the legal regime of public emergency is quite separate, under Moldovan law, from the special powers granted in the present Law. The Venice Commission thus understands that the present Law grants powers which are intended to deal with more limited, and more short-term, crises, not of the level of severity to be a "threat to the life of the nation" within the meaning of Article 15 of the ECHR. However, there are no geographic or temporal limits of an anti-terrorist operation provided for in the Law, and there is no provision on automatic expiry of the regime after a maximum period of time. The Venice Commission considers that it is important that the line between "peacetime" and "public emergency" is not blurred by the present Law and that whatever material and procedural safeguards which apply regarding the declaration of a public emergency in Moldova are not circumvented.

54. The two legal regimes thus are, and should be, kept separate. The Venice Commission nonetheless considers that it is advisable to involve Parliament, in some way, in at least certain types of anti-terrorist operations. Some form of external independent control (meeting evidence based criteria) must exist over the reasonableness of the decision to initiate the anti-terrorist operation, whoever is entrusted to initiate the operation, the Minister (which the Venice Commission considers is the preferable alternative), or the Director of the SIS. Different mechanisms of control can be envisaged – for example, court approval or the approval by some sort of parliamentary commission or sub-commission.

55. The Venice Commission notes that Moldova has a parliamentary sub-commission which has the role of overseeing the SIS. However, the effectiveness of this sub-commission is a matter for some debate (see paragraph 31 above). This is, admittedly, not an unusual situation: Moldova is by no means the only country where serious questions have been raised about the value in practice of parliamentary oversight of the security and intelligence services. Several countries have struggled, and are still struggling, to devise proper oversight mechanisms for their security and intelligence services. Nonetheless the Venice Commission recollects that, according to the

[31] CDL-AD(2016)037, Turkey - Opinion on Emergency Decree Laws Nos. 667-676 adopted following the failed coup of 15 July 2016, § 53

case-law of the ECtHR, oversight has to be effective *in practice*, and not simply exist on paper.[32] In any event, the Venice Commission considers that oversight – in the usual sense in which it is used, meaning some form of effective *post hoc* scrutiny and accountability[33] – is insufficient as regards the decision to *initiate* at least some forms of more far-reaching anti-terrorist operations. What is needed for more far-reaching anti-terrorist operations is some form of control in the sense of a parliamentary mechanism for *approval*, or *post hoc veto*, or *annulment*.

56. The Venice Commission therefore considers that, given the extent of powers granted to the CTC within the zone, the legal regime of the anti-terrorist operation should be introduced for a *limited* period of time. If this regime is introduced in respect of a particularly large geographical area (for example, for the whole region or the capital city), or extended beyond the original period of time, the legislator should consider subjecting such decisions to heightened scrutiny and introducing additional safeguards – for example, by requiring the approval of such operations by an urgent sitting of the plenary Parliament.

3. Use of lethal force; liability of the security forces

57. During a counter-terrorist operation the security forces, acting on the orders of the CTC, are allowed to use lethal force against terrorists. Thus, Article 7 (1) (e) speaks of the "the counter-terrorist intervention" by "the special purpose unit"; under Article 7 (4) (d) the Ministry of Defence is tasked with providing "the military equipment, weapons and munitions within the anti-terrorist operation". Under Article 25 (3) the CTC is preparing plans for the counter-terrorist operation, and issues "battle orders". Finally, Article 29 authorises the head of the CTC to trigger "the counter-terrorist intervention", when the "defensive" methods of solving the crisis did not work.

58. The Law does not establish the moment when a counter-terrorist intervention may be ordered by the head of the CTC, but simply refers to "the circumstances of the situation created" (Article 29 (3)). It does not define what "weapons" and "equipment" may be used in such interventions. In deciding whether a forced intervention is necessary, the CTC is guided only by the general principles formulated in Article 4 (g) and (h) of the Law, namely the principle of "priority for the protection of the rights of the persons that are being jeopardised by the terrorist activity and minimizing losses of human life", and "the principle of minimum surrender to a terrorist". Finally, Article 28 formally prevents satisfying demands of the terrorists which relate to "extradition [sic] of persons, transmission of weapons and resources the use of which might pose a risk to life and health of people, or satisfaction of political claims", as well as "exemption [of the terrorists] from liability for the offences committed by them". The question remains whether this legislative framework is adequate.

59. The Venice Commission reiterates that, in the counter-terrorist context, police operations should be "planned and controlled by the authorities so as to minimise, to the greatest extent possible, recourse to lethal force and human losses, and whether all feasible precautions in the choice of means and methods of a security operation were taken".[34] That being said, it may be difficult to set out in the law a precise rule defining what sort of concessions may be granted to the terrorists, when the authorities may stop the negotiations and intervene *manu militari*, what sort of means they may use and which precautions they should take.

60. As regards the decision to start a "counter-terrorist intervention", the ECtHR, in examining a particular counter-terrorist operation *ex post*, held that it would not "speculate on the issue of whether, as a matter of principle, it is always necessary to negotiate with terrorists and 'ransom' the lives of hostages by offering terrorists money or meeting their other requirements", and that

[32] See, *mutatis mutandis*, ECtHR, *Al-Nashif v Bulgaria*, no. 50963/99, 20 September 2002, § 136. See also *Segerstedt-Wiberg and others v. Sweden*, no. 62332/00, 6 September 2006, § 117, and CDL-AD(2015)010, Report on the Democratic Oversight of the Security Services (updated), section VIII.

[33] CDL-AD(2015)010, Report on the Democratic Oversight of the Security Services (updated), section V.A.

[34] ECtHR, *Finogenov and others v. Russia*, nos. 18299/03 and 27311/03, 20 December 2011, § 208, with further references.

"formulating rigid rules in this area may seriously affect the authorities' bargaining power in negotiations with terrorists".[35] The Venice Commission is not better equipped to devise such a rule. It may be even wiser *not* to define in the law all operational and political choices available to the security forces and to the State in general.[36] The crisis scenario envisaged should perhaps not be so narrowly prescriptive as to limit or prohibit the options available which might in certain circumstances be the most effective way of preventing ongoing terrorist activity and diffusing deadlock in hostage situations and facilitate regaining control.

61. In any case, even where a very detailed regulatory framework is in place, the law by itself cannot totally prevent errors in the planning and conduct of a counter-terrorist operation. To reduce the risk of such errors, the law may be amended as follows.

62. First, as regards the use of weapons, the Law should "incorporate in […] clear manner the principles of using force that should be no more than 'absolutely necessary,' such as the obligations to decrease the risk of unnecessary harm and exclude the use of weapons and ammunition that carried unwarranted consequences."[37] The rule prohibiting indiscriminate use of weapons not adapted to the situation may be usefully added to the Law.

63. Second, the Venice Commission has already recommended reinforcing the mechanism of parliamentary control over the routine activities of the SIS. This mechanism may also be applied to evaluate the actions of the SIS, the CTC and other State bodies involved in the counter-terrorist operation.

64. Third, the CTC and its personnel should be liable for inadequate planning and conduct of the counter-terrorist operations. Currently, Article 41 of the Law may be interpreted as providing for full immunity of security forces personnel against "forced harm to the health and belongings of terrorists", and "for the damages caused during the course" of the counter-terrorist operation. Indeed, in the course of a counter-terrorist operation the security personnel may cause harm to the terrorists (and even other persons), but only if this harm is proportionate. The Law should provide for the liability – both criminal and disciplinary – of the security personnel for *grossly disproportionate* actions which caused such harm. The State should bear civil liability in these cases. And in all cases where a security operation leads to the loss of life or limb, the case-law of the ECtHR requires a full and independent investigation into the actions of the security services.[38] The Law should be amended in these respects.

G. Limitations on media coverage

65. Article 34 gives the head of the CTC the power to censor all media reporting during a counter-terrorist operation. Under Article 35, journalists cannot interview people without the consent of the head of the CTC. They cannot provide airtime to the terrorists, nor give them the floor otherwise, for example by enabling them to articulate their claims and ideas. The journalists cannot disseminate information about the forces involved in the counter-terrorist operation, their position, etc. These limitations may however interfere with the freedom of the press, guaranteed by Article 10 of the ECHR. Indeed, the States have a margin of appreciation when regulating the speech in the context of fight against terrorism.[39] However, this margin is not all-embracing.

---

[35] Ibid, § 223

[36] As the ECtHR noted in *Finogenov*, cited above, "even if necessary regulations [on the conduct of the anti-terrorist operation] did exist, they probably would be of limited use in the situation at hand, which was totally unpredictable, exceptional and required a tailor-made response" (§ 230). That being said, a distinction should be made between routine police operations (which should be better regulated as to the conditions of the use of force and the weapons and means used) and situations of a major terrorist crisis, as the one described in *Finogenov*.

[37] ECtHR, *Tagayeva and Others v. Russia*, nos. 26562/07 et al., 13 April 2017, § 598.

[38] See, e.g. *Mustafa Tunç and Fecire Tunç v. Turkey* [GC], no. 24014/05, 14 April 2015, *Armani Da Silva v. the United Kingdom*, no. 5878/08, ECHR 2016.

[39] Thus, in the 1980s, the former European Commission on Human Rights accepted limited controls on journalist interviews with terrorists – see *Brind and Others v. the United Kingdom*, no. 18714/91, decision of 9 May 1994.

66. It might be legitimate to keep secret certain *technical aspects* of the anti-terrorist operation *while the crisis is on-going* in order not to jeopardise the operations. However, the authorities should not be tempted nor allowed to use secrecy rules to keep their actions from public scrutiny. It is the main role of journalists, as "public watchdogs", to reveal unjustified or unlawful actions[40] and it is a right of the public to be informed about them.

67. Limitations on media coverage are easier to justify if they are narrowly tailored: they should be of a short duration, be applied to a limited geographical zone, and relate to tactical aspects of the on-going counter-terrorist operation and similar "secret" information. Regrettably, some of the formulas used in Article 34 suggest that the prohibitions set out in the article are not limited to the specific zone ("in particular during the anti-terrorist operation"). The blanket prohibition of taking interviews is also problematic (since not every interview will disclose to the terrorists sensitive information).

68. Some of the limitations under Articles 34 and 35 concern the general reporting about the terrorist crisis, even if such reporting does not disclose any "secret" information, and touches upon matters of public interest. Limitations in this respect are more problematic. The intent of the legislator to limit the reporting from a crisis zone may be understood, since terrorism feeds on fears and anxiety of the general public, which is sometimes fuelled by the irresponsible media reporting. However, to promote responsible journalism it is more appropriate to make recourse to self-regulations in order to limit the "media outreach" of the terrorists. As noted by the Committee of Ministers, "self-regulation as the most appropriate mechanism for ensuring that media professionals perform in a responsible and professional way needs to be made more effective in times of crisis".[41]

69. In the opinion of the Venice Commission, the Law may establish a *strong presumption* in favour of non-disclosure of such information during the crisis, but should provide that the "public interest defence" is available to the journalists (in this Law or elsewhere).

70. Article 45 provides for the liability for "dissemination of information materials which call for carrying out terrorist activities or support them". Dissemination of such information may lead to "termination or discontinuation" of the activity of the media outlet concerned, or temporary suspension of its activities, and forfeiture of the unsold part of the print. The Venice Commission recalls that the Law gives its own definition of "terrorist activity", which goes beyond the definition of "terrorism" and "terrorist offences" formulated in the Criminal Code. Although the definition of the "terrorist offences" in the Criminal Code and "terrorist activity" in the Law are very similar, they are not identical, which increases the risk of an overly broad interpretation of this term, especially under the limb of "support", and "public justification of terrorism" (which makes part of the definition of "terrorist activities" given by the Law itself in Article 3).

71. It is difficult to assess the proportionality of this norm *in abstracto*, without the context of a particular case. The Venice Commission is ready to acknowledge that a media outlet openly calling for violent attacks against civilians and/or government institutions may need to be suspended and even closed. However, the authorities should not give an overly large definition of "support" or "public justification" of terrorism in order to hush legitimate criticism of their policies.[42] This risk is exacerbated by the fact that Article 45 provides for only two sanctions – definitive "discontinuation of activities" (= liquidation) and temporary suspension of activities of the media outlet concerned. As the Venice Commission noted, "temporary shutdown is a very serious interference and may endanger proper functioning of a media outlet and even its very existence".[43] This is obviously even more true in respect of the closing down of the outlet.

---

[40] See ECtHR, *Stoll v. Switzerland* [GC], no. 69698/01, 10 December 2007, §§ 108 et seq.

[41] Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis (26 September 2007), p. 25

[42] See *Fatullayev v. Azerbaijan*, no. 40984/07, 22 April 2010; *Belek and Velioğlu v. Turkey*, no. 44227/04, 6 October 2015.

[43] CDL-AD(2015)004, Opinion on the draft Amendments to the Media Law of Montenegro, § 23

72. In order to reduce the likelihood of a disproportionate interference with the freedom of expression, this Article should provide for a more gradual response to publications which may contain elements of "justification" or "support" of terrorism: even where the media outlet overstepped the permissible bounds, it should not be necessarily struck immediately with as harsh a sanctions as a temporary shut-down, which may tantamount to *de facto* liquidation, or with *the de jure* liquidation). The law must provide for additional – less harsh – sanctions which may be sufficient to deter media outlets from expressing "support" to terrorists.

H. Black lists of suspected terrorists

73. Article 8 (2) (i) provides that the Anti-Terrorist Centre of the SIS will create and maintain a databank of terrorist organisations and "persons involved in the work of such organizations, natural and legal persons providing terrorists with support including financial one". Article 10 (1) (d) – which speaks of the persons entering, crossing or leaving the territory of Moldova – stipulates that "the list of persons, groups and entities involved in terrorist activities shall be drawn up, updated by the Security and Intelligence Service and published in the Official journal of the Republic of Moldova)." In essence, it means that the SIS will run "black lists" of the suspected terrorists – a general one (under Article 8) and one for the border controls (under Article 10).

74. As regards the black-list under Article 10, it is composed on the basis of sources, enumerated in Article 10 (2), namely: the lists of terrorists and terrorist organisations approved by the international organisations and by the EU bodies, the decisions of the domestic courts and the decisions of foreign courts. This list is public – thus, the person concerned may know about being on the list. Three observations are called for in respect of Article 10.

75. First, the EU/UN and other similar blacklisting systems have been criticised for the lack of legal certainty (even if improvements have been made in the past years), and for the lack of legal remedies available to the persons on this list. In the case *Nada v. Switzerland*[44] the ECtHR examined the prohibition for an Egyptian national on entering or transiting through Switzerland due to the fact that his name had been put on a black list of terrorists by the UN Security Council's Sanctions Committee. The ECtHR held that there had been a violation of Articles 8 and 13 because of the blind reliance of the Swiss authorities on the UN SC black list, and because of the fact that the applicant did not have any effective remedy to obtain the removal of his name from this list.

76. It is even more problematic to automatically rely on decisions of foreign courts . The Venice Commission has already been confronted with situations where criminal law and judicial practice in a given country give a very broad definition of "terrorism".[45] There is a risk that ordinary criminal offenders or political dissidents are labelled as "terrorists" – and that is by a final judgment of a competent foreign court. As regards the possibility of appealing to have one's name removed from the black list, the Law provides that final court decisions rendered by Moldovan or foreign courts cannot be challenged. The Law itself does not mention any legal remedy available for persons put on the list.

77. To the extent that Article 10 of the Law deals with aliens trying to enter the country, international refugee law may come into play: if an asylum seeker trying to enter the territory of Moldova was convicted for "terrorism" in his/her home country, and if, in this country, there exists a serious risk for his or her life and limb, "non-admitting" this person to the national territory may be problematic from the point of view of the 1951 Convention on Refugees (and also Articles 2 and 3 of the ECHR).[46] The Moldovan courts should therefore have the power of assessing

[44] [GC], no. 10593/08, 12 September 2012
[45] See CDL-AD(2016)002, Opinion on articles 216, 299, 301 and 314 of the Penal Code of Turkey, §§ 98 et seq., and CDL-AD(2016)037, Turkey - Opinion on Emergency Decree Laws Nos. 667-676 adopted following the failed coup of 15 July 2016, §§ 128 et seq.
[46] See *Chahal v. the United Kingdom* [GC], no. 22414/93, 15 November 1996

whether the offences imputed to the person entering, crossing or leaving the territory of Moldova were indeed "terrorist" offences within the meaning of international conventions and of the relevant Moldovan legislation. In addition, Article 10 is formulated as if it also concerns Moldovan citizens, and in this case Article 2.2 of Protocol No. 4 to the ECHR must be respected.

78. In the opinion of the Venice Commission, the "black-listing" mechanism provided by Article 10 should be supplemented. The legislator should give the person concerned the right to ask to be removed from the list, and it should be for the Moldovan courts to decide, in the final instance, whether non-admission to the country (or any other possible consequences of being on the list) are compatible with the Moldova's other international obligations.

79. As regards the database of terrorists and terrorist organisations provided by Article 8, it is unclear how it is composed and what purpose it serves. The Law does not provide for any possibility of challenging the content of this database. So, there are no guarantees preventing innocent people from being included in this database by mistake or even malice. A lot will depend on what use the SIS may make of this database. As a minimum guarantee against abuses, there must be an effective control of this database and its use both by a competent parliamentary committee (or a mixed expert body) supervising the activities of the SIS, and by the courts in cases where the inclusion in the database led to an interference with somebody's rights.

I. Liquidation of entities involved in "terrorist activities"

80. Article 43 establishes liability of legal persons for "carrying out terrorist activity". Article 44 establishes "liability of non-governmental organizations or religious associations, other institutions for carrying out terrorist activities". The need for two separate articles is not clear – NGOs and other institutions are legal persons, so it should suffice to have one article for both purposes.

81. The decision to liquidate the entity is taken by an "irrevocable decision of the court", upon application by the SIS or by the prosecution. It is not clear what "irrevocable" means in this context. It is necessary to indicate that usual channels of appeal should be available to the interested parties.

82. Liquidation of a legal entity is ordered if it is involved in a "terrorist activity", as defined in Article 43 itself.[47] This is another example of terminological inconsistencies in the Law – the definition of a "terrorist activity" under Article 43 is not identical to the definition of "terrorist activity" in Article 3 (which is, in turn, larger than the definition of "terrorism" and "terrorist offences" in the Criminal Code). In the opinion of the Venice Commission, the Law must make it clear that the liquidation is possible only in relation to the participation in "terrorist offences", as defined by the Criminal Code; the notion of "terrorist activity" is misleading and must not be employed here.[48] Liquidation must also be ordered only if it may be considered as necessary in a democratic society.

83. Some of the formulas used in Article 43 and 44 need to be further clarified – in particular, as regards terrorist offences which "have been allowed, authorized, approved or used by the body or person empowered with leading roles within the legal entity". The Venice Commission recalls that there should be a meaningful link between terrorist offences and the acts of the executives of the legal entity concerned.[49]

[47] "Where in the name or on behalf of the legal person thereof is being organized, prepared, financed or committed a terrorist offence, as well as where such actions have been allowed, authorized, approved or used by the body or person empowered with leading roles within the legal entity thereof".

[48] At the same time, the Venice Commission acknowledges that the definition of "terrorist activities" may be useful for delimiting the mandate of the SIS, which may be broader.

[49] See CDL-AD(2016)037, Turkey - Opinion on Emergency Decree Laws Nos. 667-676 adopted following the failed coup of 15 July 2016, §§ 128 et seq.

J. Burial of bodies of terrorists

84. Article 32 provides that bodies of terrorists killed in the counter-terrorist operations are not given to their relatives, and that the place of burial is not disclosed to them. Even if the government wishes understandably to avoid the situation where the burial of terrorists becomes an opportunity for a propaganda coup for the terrorist organisation, this measure seems excessive. A similar question was discussed by the ECtHR in the case of *Sabanchiyeva and Others v. Russia*,[50] where the Court found a violation of Articles 8 and 13 on account of an automatic refusal to return the bodies of presumed terrorists to their families, without taking into account the individual circumstances of each of the deceased and those of their family members.

85. The central question is how the bodies of "terrorists" may be distinguished from the bodies of innocent bystanders or even hostages, killed by accident during the counter-terrorist operation. During the visit to Chisinau, the rapporteurs were explained that, under the Moldovan legislation, it is possible to complete a criminal trial even in respect of a deceased person, and thus establish whether that person was a terrorist or not. The idea of a trial where the defendant cannot defend him- or herself is open to criticism when the law does not provide for a specially adapted procedure ; in any event, matters related to the burial of bodies should be decided by a court with the participation of all interested parties (like the next of kin of the "supposed terrorist").

III. Conclusion

86. Law no. 120, adopted in 2017, establishes principles and rules of the fight against terrorism, and the institutional arrangements in this sphere. The Venice Commission reiterates that a State needs effective intelligence and security services: intelligence is thus an inescapable necessity for modern governments. The Republic of Moldova, in the face of the terrorist threat, is entitled to take extraordinary measures. However, those measures should be mutually coherent, foreseeable, and compatible with the human rights obligations which Moldova has under the international and European human rights law. From this perspective, Law no. 120 needs a thorough revision, and its relation with other relevant legislation (in particular the Criminal Procedure Code and Law no. 59 on the special investigative activities) should be specified more clearly.

87. The Venice Commission is confident that such revision may be done without affecting the necessary effectiveness of anti-terror mechanisms and powers. Amongst the most important amendments, the Venice Commission recommends the following:

- The list of measures which the Secret Intelligence Service may take within the "prevention" mandate (insofar as they may affect private persons) and of the corresponding obligations of private persons, must be reviewed. These measures should be described with due precision as to their material scope, and the Law must provide that some of those measures need an external authorisation (a court warrant, a decision by the prosecution, etc.) and specify the measures and the relevant procedures in detail.

- The Speaker of Parliament should not have the power to coordinate anti-terrorist activities; this should be a prerogative of the executive. Instead, a clear and unambiguous oversight procedure must be put in place: the parliamentary control mechanism should be reinforced, involving either the sub-commission on the Secret Intelligence Service, or a mixed expert body, both with strong presence of the opposition. In addition to the examination of general reports, such bodies should have access to the specific files. A proper record-keeping system should be put in place within the Secret Intelligence Service.

[50] No. 38450/05, 6 June 2013

- Anti-terrorist operations should be of limited duration and cover a limited geographical zone; any extension of the zone or of the duration of the operation must be accompanied by increased parliamentary control.

- The Law should provide for criminal and disciplinary liability of the security personnel for grossly disproportionate actions and for inadequate planning and conduct of the anti-terrorist operations. The State should bear civil liability in cases of harm caused by such disproportionate actions. Indiscriminate use of weapons not adapted to the situation should be prohibited under the Law, and the actions of the security personnel which resulted in the loss of life or limb should be subject to an independent and effective investigation.

- Limitations on the media reporting during a terrorist crisis should be of short duration, and concern only certain specific types of information (i.e. on the forces involved in the counter-terrorist operations, their position, methods, and alike), in line with the principle of proportionality. The journalists should be free to inform the public about the general situation during the terrorist crisis, subject to their duties under the European Convention on Human Rights; principles of responsible media coverage may be defined in the self-regulations.

- "Black lists" of terrorists should not rely blindly on decisions of foreign courts and governments. An effective appeal process accessible to all affected persons should be put in place. The Moldovan courts should be able to verify whether the person concerned is indeed a "terrorist" within the meaning of the Moldovan legislation and under the international law. Expulsion and extradition of presumed "terrorists" is possible only if it does not contradict the obligations of Moldova under the 1951 Convention on Refugees and the European Convention on Human Rights.

88. The Venice Commission remains at the disposal of the authorities of the Republic of Moldova for further assistance in this matter.