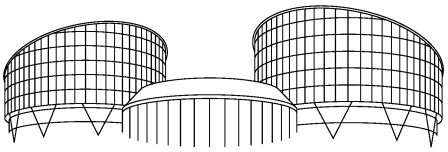

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF SZABÓ AND VISSY v. HUNGARY

(Application no. 37138/14)

JUDGMENT

STRASBOURG

12 January 2016

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Szabó and Vissy v. Hungary,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Vincent A. De Gaetano, *President,*
András Sajó,
Boštjan M. Zupančič,
Nona Tsotsoria,
Paulo Pinto de Albuquerque,
Krzysztof Wojtyczek,
Iulia Antoanella Motoc, *judges,*

and Fatoş Aracı, *Deputy Section Registrar,*

Having deliberated in private on 14 April and 15 December 2015,

Delivers the following judgment, which was adopted on the last-mentioned date:

PROCEDURE

1. The case originated in an application (no. 37138/14) against Hungary lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by two Hungarian nationals, Mr Máté Szabó and Ms Beatrix Vissy ("the applicants"), on 13 May 2014.

2. The applicants were represented by Mr L. Majtényi, a lawyer practising in Budapest. The Hungarian Government ("the Government") were represented Mr Z. Tallódi, Agent, Ministry of Justice.

3. The applicants complained under Article 8 of the Convention that they could potentially be subjected to unjustified and disproportionately intrusive measures within the framework of "section 7/E (3) surveillance" (see paragraphs 10-12 below), in particular for want of judicial control. In their view, the latter issue also constituted a violation of their rights under Articles 6 and 13 of the Convention.

4. On 12 June 2014 the application was communicated to the Government.

5. On 27 August and 1 September 2014, respectively, Privacy International and Center for Democracy and Technology, both non-governmental organisations, were granted leave to make written submissions (Article 36 § 2 of the Convention and Rule 44 § 3 of the Rules of Court).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

6. The applicants were born in 1976 and 1986 respectively and live in Budapest.

7. When introducing the application, the applicants were staff members of *Eötvös Károly Közpolitikai Intézet*, a non-governmental, "watchdog" organisation voicing criticism of the Government. The subsequent employer of one of the applicants was subjected to financial control measures by the Government in 2014, which according to the applicants verged on vexation.

8. Act no. CXLVII of 2010 defines combating terrorism as one of the tasks of the police. Within the force, a specific Anti-Terrorism Task Force ("*TEK*") was established as of 1 January 2011. Its competence is defined in section 7/E of Act no. XXXIV of 1994 on the Police, as amended by Act no. CCVII of 2011 (the "Police Act").

9. Under this legislation, TEK's prerogatives in the field of secret intelligence gathering include secret house search and surveillance with recording, opening of letters and parcels, as well as checking and recording the contents of electronic or computerised communications, all this without the consent of the persons concerned.

10. The authorisation process for these activities is dependent on the actual competence exercised by TEK, namely whether it is within the framework of secret surveillance linked to the investigation of certain specific crimes enumerated in the law (section 7/E (2)) or to secret surveillance within the framework of intelligence gathering for national security (section 7/E (3)).

11. Whereas the scenario under section 7/E (2) is as such subject to judicial authorisation, the one under section 7/E (3) is authorised by the Minister in charge of justice, (i) in order to prevent terrorist acts or in the interests of Hungary's national security or (ii) in order to rescue Hungarian citizens from capture abroad in war zones or in the context of terrorist acts.

12. "Section 7/E (3) surveillance" takes place under the rules of the National Security Act under the condition that the necessary intelligence cannot be obtained in any other way. Otherwise, the law does not contain any particular rules on the circumstances in which this measure can be ordered, as opposed to "section 7/E (2) surveillance", which is conditional on the suspicion of certain serious crimes. The time-frame of "section 7/E (3) surveillance" is 90 days, which can be prolonged for another 90-day period by the Minister; however, the latter has no right to know about the results of the ongoing surveillance when called on to decide on its prolongation. Once the surveillance is terminated, the law imposes no specific obligation on the authorities to destroy any irrelevant intelligence obtained.

13. The applicants filed a constitutional complaint on 15 June 2012, arguing in essence that the sweeping prerogatives under section 7/E (3) infringed their constitutional right to privacy. They emphasised that the legislation on secret surveillance measures for national security purposes provided fewer safeguards for the protection of the right to privacy than the provision on secret surveillance linked to the investigation of particular crimes. They pointed out that (i) "section 7/E (2) surveillance" was always linked to a particular crime and could only be ordered for the purposes of identifying or locating suspects, whereas "section 7/E (3) surveillance" was not linked to any particular crime; (ii) "section 7/E (2) surveillance" was always ordered by the court, whereas "section 7/E (3) surveillance" was authorised by the government minister in charge of justice; (iii) the decision on ordering "section 7/E (2) surveillance" was subject to detailed reasoning, whereas no reasoning was included in the minister's decision on ordering "section 7/E (3) surveillance"; and (iv) under the legislation relating to "section 7/E (2) surveillance", all collected but irrelevant information had to be destroyed within eight days, unlike in the case of "section 7/E (3) surveillance".

14. On 18 November 2013 the Constitutional Court dismissed the majority of the applicants' complaints. In one aspect the Constitutional Court agreed with the applicants, namely, it held that the decision of the minister ordering secret intelligence gathering had to be supported by reasons. However, the Constitutional Court held in essence that the scope of national security-related tasks was much broader that the scope of the tasks related to the investigation of particular crimes. For the purpose of national security, the events of real life were examined not for their criminal law relevance; therefore they might not necessarily be linked to a particular crime. Furthermore, in the context of national security, the external control of any surveillance authorised by the minister was exercised by Parliament's National Security Committee (which had the right to call the minister to give account both in general terms and in concrete cases) and by the Ombudsman, and that this scheme was sufficient to guarantee respect for the constitutional right to privacy of those concerned. Finally, the Constitutional Court was of the opinion that the National Security Act, which applies to "section 7/E (3) surveillance", contained general provisions on *ex officio* deletion of any data unnecessary for achieving the aim underlying the gathering of intelligence.

15. This decision was published in the Official Gazette on 22 November 2013.

II. RELEVANT DOMESTIC LAW

16. Act no. XXXIV of 1994 on the Police ("the Police Act") provides as relevant:

Section 1

"(2) The police – within the scope of its duties as prescribed by the Fundamental Law of Hungary, by this Act and by other laws for preventing and combating crimes, administrating and policing – ...

15. ... within the territory of Hungary ...

a) tracks terrorist organisations,

b) prevents, tracks and repels any attempts of individuals, groups or organisations to carry out terrorist acts and impedes the commission of any crimes by them,

c) impedes the promotion of the operation of terrorist organisations by individuals, groups or organisations through providing financial or other support."

Section 7/E

"(1) The anti-terrorist organ does not exercise any investigatory competence. It:

a) fulfils the tasks prescribed in section 1 subsection (2) point 15, and within these tasks ...

ad) – within the framework of the fight against terrorism and in order to safeguard the national security interests of Hungary – prevents, tracks and repels any attempts to carry out terrorist acts (*terrorcselekmény*) in Hungary. ...

d) on the basis of the decision of the Minister responsible for policing as endorsed by the Minister responsible for foreign affairs – in line with the rules of international law – contributes to rescuing Hungarian citizens who are – outside the territory of Hungary – in distress due to an imminent and life-threatening danger of act of war, armed conflict, hostage-taking or terrorist action; to ensuring their safe return to Hungary and to carrying out their evacuation; to this end it cooperates with the Member States and the organs of the European Union, with the organs of the North Atlantic Treaty Organization, with the related international organisations and with the authorities of the concerned foreign country.

e) acquires, analyses, assesses and forwards information relating to foreign countries or being of foreign origin which is required for fulfilling the task prescribed in section d) above.

(2) The anti-terrorist organ may – for the purpose of fulfilling its tasks prescribed in subsection (1) point a) sub-points aa) to ac) and in point c) – perform secret intelligence gathering in line with the provisions of Chapter VII of the Act on Police.

(3) The anti-terrorist organ may – for the purpose of fulfilling its tasks prescribed in subsection (1) point a) sub-point ad) and in point e) – perform secret intelligence gathering in line with the provisions of sections 53-60 of Act no. CXXV of 1995 on the National Security Services (the "Nbtv."), in the course of which it may request and handle data according to the provisions of sections 38-52 of Nbtv. The secret intelligence gathering provided in section 56 points a)-e) of Nbtv. is subject to authorisation of the Minister responsible for justice."

The crime of "terrorist act" (*terrorcselekmény*) is defined in section 261 of the Old Criminal Code and sections 314 to 316 of the New Criminal Code.

17. Act no. CXXV of 1995 on the National Security Services (the "National Security Act", "Nbtv.") contains the passages below.

Under section 11(5), complaints about the activities of the anti-terrorist organ shall be investigated by the Minister of Home Affairs who shall inform the complainants of the outcome of the investigations and of the relevant measures within 30 days (this deadline may, on one occasion, be extended by another 30 days).

Section 14(4) contains provisions concerning the relevant competences of the National Security Committee. In exercising parliamentary supervision, the Committee is entitled to request information from the Minister and the directors of the national security services about the country's national security situation and the functioning and activities of the services (sub-section (a)).

In individual complaint procedures, where a complainant does not accept the results of the investigation under section 11(5), the Committee may investigate complaints alleging unlawful activities on the part of the National Security Services if, under the affirmative vote of at least one third of the Committee members, the gravity of the complaint justifies an investigation. In investigating a complaint the Committee shall examine the complaint at issue and may request the Minister to submit his opinion on the case. If the Committee is of the view that the operation of the Services has been unlawful or abusive, it may request the Minister to conduct investigations and to inform the Committee of the results of the investigations or may itself carry out fact-finding investigations if it has the impression that the operation of the Services is contrary to the relevant laws. In carrying out the fact-finding investigations, the Committee may inspect the relevant documents in the records of the National Security Services and may hear staff members of the National Security Services. Relying on the findings the Committee may invite the Minister to take the necessary actions.

Section 43

"The National Security Services may use data having come to their knowledge exclusively for the purpose that corresponds to the legal basis for ordering their acquisition, except

a) if the data are indicative of the commission of a criminal act and forwarding the data is legally allowed, or

b) if they substantiate an obligation to inform another National Security Service and the party receiving the data is itself authorised to obtain them."

Section 44

"(1) For the purpose of fulfilling their tasks the National Security Services may request data from each other and are obliged to provide data to each other in line with the provisions of this Act.

(4) The bodies requesting data disclosure shall be responsible for the management of data disclosed to them according to the provisions of this Act and the data

management legislation; they shall register the data they receive and their utilisation and, upon request, they shall inform the National Security Service thereof."

Section 45

"(1) The National Security Services may, under an international obligation, transfer personal data to foreign data processing authorities within the framework of laws on protection of personal data."

Section 50

"(2) Personal data processed by the National Security Services shall be deleted immediately if

a) the deadline specified in subsection (1) has expired;

b) deletion was ordered by a court in data protection proceedings;

c) processing of the data is unlawful;

d) the conditions specified in section 60 (2) are met;

e) processing of the data became manifestly unnecessary."

Section 53

"(2) The National Security Services may apply the special means and methods of secret intelligence gathering only if the intelligence needed for the performance of the tasks laid down in the present Act cannot be obtained in any other way."

Section 56

"The National Security Services may, under an external permission

a) search a dwelling secretly and record by means of technical equipment what they perceive;

b) keep a dwelling under surveillance by means of technical equipment and record what they perceive;

c) open and check postal mail and any closed parcel belonging to an identifiable person and record their contents by means of technical equipment;

d) detect the content of communications transmitted by electronic communications network and record it by means of technical equipment;

e) detect the data transmitted by or contained on a computer or network, record it by means of technical equipment and use it."

Section 57

"(1) The motion to obtain permission for secret intelligence gathering as specified in section 56 may be submitted by director generals of the Information Authority, the Constitution Protection Authority, the Military National Security Service and – in order to carry out its task specified in section 8 (1) f) above – the Special Service for National Security.

(2) The motion shall contain:

a) the premises of the secret intelligence gathering, the person(s) concerned identified by name or as a range of persons, and/or any other information capable of identifying such person or persons;

b) specification of the secret intelligence gathering and reasoning substantiating its necessity;

c) the date of the beginning and the end of the activity;

d) in the case of a motion to obtain permission specified in section 59 below, reasoning why the requested intelligence is absolutely necessary in the specific case for the successful functioning of the National Security Service."

Section 58

"(3) The ... Minister in charge of justice ... decides [on the motion] within 72 hours to be counted from the motion's submission ... [he] grants permission or, in case of an ill-founded request, rejects it. No appeal lies against the decision.

(4) Unless this law stipulates otherwise, the authoriser allows the secret intelligence gathering for a period of a maximum of 90 days upon each request. In justified cases and upon a motion from the director generals, this time limit may be extended by 90 days, unless this law stipulates otherwise.

(6) The authoriser does not inform the person concerned about the proceedings or about the occurrence of secret intelligence gathering."

Section 59

"(1) The directors of the National Security Services themselves may [exceptionally] authorise the secret gathering of information within the meaning of section 56 at the latest until the decision given [by the Minister] if the external authorisation procedure entails such delay as obviously countering, in the given circumstances, the interests of the successful functioning of the National Security Service."

Section 60

"(1) Secret intelligence gathering based on external permission shall be discontinued immediately if

a) it achieved its aim defined in the permission;

b) its continuation does not promise any results;

c) its time-limit has been expired without extension;

d) the secret intelligence gathering is unlawful for any reasons whatsoever.

(2) In the framework of the special procedure defined in section 59 (1), secret intelligence gathering shall also be discontinued immediately if the authoriser does not permit its continuation. In that case, the data obtained by secret intelligence gathering shall be destroyed immediately, according to the laws regulating the deletion of qualified data."

Section 74(a) defines the notion of national security interests in the following terms:

"Securing the sovereignty and protecting the constitutional order of Hungary and, within that framework,

aa) obtaining intelligence on aggressive efforts targeted against the independence and territorial integrity of the country,

ab) obtaining intelligence on and combating covert efforts violating or threatening the political, economic or defence interests of the country,

ac) obtaining information of foreign relevance or origin required for government decisions,

ad) obtaining intelligence on and combating covert efforts aimed at altering or disturbing by unlawful means the country's constitutional order guaranteeing respect for fundamental human rights, pluralist representational democracy, the constitutional institutions and

ae) obtaining intelligence on and combating acts of terrorism, illegal arms and drugs trafficking, and illegal trafficking in internationally controlled products and technologies;"

18. Act no. CXI of 2011 on the Commissioner for Fundamental Rights ("Ajbt.") provides as follows:

Under section 18 (1) f), law enforcement organs – including the anti-terrorist organ – are authorities subject to investigation by the Ombudsman. There is only one limitation on the investigations conducted by the Ombudsman: the report drafted on the secret intelligence activities of organs authorised for using secret intelligence devices shall not contain data from which the conclusion can be drawn that in the given case secret intelligence activities were or have been carried out by the organ [cf. section 28(3)]. The Commissioner for Fundamental Rights shall annually submit a report to Parliament about the investigated cases and may – except for proposals for amendments – request Parliament to investigate any given case. Where the finding of an abuse or maladministration affects classified data, the Commissioner for Fundamental Rights shall – simultaneously with the annual report or, if the abuse or maladministration is very grave or affects a great number of natural persons, before the submission of the annual report – submit the case to the competent parliamentary committee in a report classified according to the Act on the Protection of Classified Data.

The applicants submitted a statement obtained from the Commissioner's Office on 9 July 2014, according to which the Commissioner had never enquired into the field of secret surveillance measures.

19. Act no. CLI of 2011 on the Constitutional Court provides as follows:

Section 26 (1)

"Persons or organisations affected by a particular case may, under Article 24 (2) c) of the Fundamental Law, submit a constitutional complaint to the Constitutional Court where due to the application in the related court proceedings of a piece of legislation contravening the Fundamental Law,

a) their rights enshrined in the Fundamental Law have been violated, and

b) legal remedies have been exhausted or no remedy exists.

(2) By way of derogation from subsection (1), such Constitutional Court proceedings may, exceptionally, also be initiated where

a) the injury originated directly from the application or becoming effective of a provision contravening the Fundamental Law, without a court decision, and

b) no procedure to redress the injury is available or the available remedies have already been exhausted by the complainant. ...”

Section 27

“Against a judicial decision contravening the Fundamental Law within the meaning of Article 24 (2) d.) of the Fundamental Law, a person or organisation affected by the particular case may file a constitutional complaint with the Constitutional Court where the decision on the merits of the case or another decision terminating the judicial proceedings

a) has violated the complainant’s rights enshrined in the Fundamental Law, and

b) the complainant has already exhausted the legal remedies or no legal remedy exists.”

20. Decision no. 32/2013. (XI.22.) AB of the Constitutional Court establishing the constitutional requirement to be met in respect of section 58 (3) of Nbtv. and rejecting the related constitutional complaint contains the following passages:

“... 1. The Constitutional Court finds that ... in order to make the external control effective, the decision of the Minister responsible for justice ... authorising secret intelligence gathering must be supplied with reasons. ...

[42] 1.1. The regulations in force specify two types of secret intelligence gathering: secret surveillance linked to the investigation of particular crimes and secret surveillance not linked to the investigation of particular crimes. ...

[47] 1.2. Secret surveillance not linked to the investigation of particular crimes is either not subject to external authorisation [sections 54-55 of Nbtv.] or is subject to external authorisation [sections 54-55 of Nbtv.] In cases specified in the Act authorisation means authorisation by a judge or by the Minister of Justice.

[48] According to the reasoning of Nbtv., from international practice several examples can be mentioned for States making a distinction between intelligence gathering linked to the investigation of particular crimes (including the closely related fields of crime prevention and crime detection) and intelligence gathering carried out for national security purposes.

[49] On the basis of this principle, a system of divided authorisation has been adopted in the Act. For the purpose of detecting actual criminal offences, secret intelligence gathering is authorised – similarly to the solution applied in the Act on the Police – by a judge designated for the task by the President of the Budapest High Court, whereas section 56 activities carried out in the course of general intelligence gathering shall be authorised by the Minister of Justice. ...

[51] Section 53 (2) of Nbtv., according to which secret intelligence gathering may only be carried out if the data required to perform the statutory tasks cannot be obtained in any other manner, shall apply to both cases. ...

[62] Under section 14 (4) of Nbtv. Parliament's National Security Committee shall exercise control over the authorisation process of the Minister of Justice. ...

[69] 2. Secret intelligence gathering governed by Nbtv and not linked to the investigation of particular crimes ... has not been examined by the Constitutional Court yet. However, in its decision no. 2/2007. (I. 24.) AB (henceforth: Abh.1.) the Constitutional Court specified the general aspects under which secret intelligence gathering and secret surveillance are acceptable in a democratic, rule-of-law State.

[70] Since the content of Article B) (1) of the Fundamental Law is identical to the content of Article 2 (1) of the former Constitution, and since from the rules of interpretation applicable to the Fundamental Law no conclusion contrary to the above opinion of the Constitutional Court can be inferred, the statements of principle made on the necessity and proportionality of secret intelligence gathering can be maintained.

[71] The Constitutional Court has also taken into consideration the Strasbourg Court's jurisprudence, as recalled in its former decisions. Cases related to "covert investigations" were examined by the Court in light of the Convention provisions set forth in Article 8 which protects the right to respect for private life. In its judgments the Court held that in a democratic society the rights enshrined under Article 8 § 1 can only be restricted within the limits specified in paragraph 2, that is only for the purposes specified in that provision and only in case the necessity of the restriction is justified.

[72] Lawfulness under the Court's case law does not merely require that a given restriction be specified under the law. The phrase "in accordance with the law" requires that the regulation itself should meet the rule-of-law principles. Since secret intelligence gathering does, per definition, exclude the possibility of an effective remedy, it is imperative that the process authorising such information gathering should contain sufficient guarantees for the protection of the rights of the individuals. Therefore, the use of secret intelligence gathering must be subject to a three-stage control: when the interference is ordered, while the interference is carried out and when the interference is terminated. Control must be exercised by "bodies" independent of the executive power. First of all, only constant, continuous and mandatory control can guarantee that in a given case the requirement of proportionality is not violated ....

[73] In its judgments the Court laid down the minimum requirements to be met by a legal regulation on the use of secret intelligence devices. The Court emphasised that since the interference with the fundamental rights is secret and since the use of such devices provides "unpredictable" opportunities for the executive power, it is indispensable that the procedures themselves provide sufficient guarantees for the observance of the rights of the individuals. Therefore States must create precise and detailed rules that can be abided by and accessed by the citizens. From the legal regulation the competence of the authority applying such devices, the essence of the measures and the manner of their practice should be clear and apparent. As to the requirement of the clarity of rules the Court also pointed out that the laws should specify the cases and circumstances which warrant such interference and the conditions of the interference. As a minimum guarantee the laws should determine the criteria based on which the scope of persons potentially affected can be determined and should contain provisions regulating the documentation of the use of secret intelligence devices and specifying the rules applicable to the protection and destruction of the documentation. As to decision-making on the application of secret intelligence devices, an excessively wide margin of appreciation may not be granted

for the authorities (e.g. *Valenzuela Contreras v. Spain* (58/1997/842/1048)). As to the application of secret intelligence devices, the requirement that access to the information by outside persons should be restricted serves as an additional guarantee (e.g. *Kopp v. Switzerland* (13/1997/797/1000) 25 March 1998).

[74] Use for a particular purpose means that secret intelligence devices may only be used for reasons specified in Article 8 § 2 .... Compliance with the necessity test is closely linked to this issue. It is a basic requirement that any interference should be justified by pressing public interest and should be proportionate both to the danger needed to be countered and to the injury caused.

[75] An examination of these issues should not be confined to scrutinising whether the statutory conditions laid down for the restriction meet the necessity-proportionality test but should also extend to examining the necessity of the use of secret intelligence devices in the particular case. As to the requirement of necessity it is of paramount importance that any use should only take place in case of "aggravated" (serious) threat and only in case the traditional investigative means and devices prove to be inefficient in the particular circumstances of a case; moreover, any use of the secret intelligence devices should take place according to a strict procedure that can be known in advance ...

[76] From the Convention and the relevant case law of the Court the Constitutional Court has concluded that national security, public security and the prosecution of crime are interests for which even covert investigations – which amount to serious law-restricting devices – can be used where the above specified criteria are met.

[77] 3. The Constitutional Court has examined the contested provision within the confines of the complainants' complaint. The complainants challenged the anti-terrorist organ's secret intelligence gathering activities carried out for purposes other than prosecuting crime. They alleged non-compliance with the Fundamental Law of the contested provision by alleging that the provision at issue allowed for the anti-terrorist organ's secret intelligence gathering under Nbtv. – while Nbtv. contained no guarantees for the observance of the fundamental rights at issue.

[78] The complainants did not make a distinction between the various stages of the secret intelligence gathering (ordering, carrying out and terminating the interference) but picked out some elements of the application [of this measure] and complained about those elements. As to the ordering of the interference they complained that the permission of the Minister responsible for justice did not constitute a sufficient guarantee, in particular in view of the fact that the grounds on which the request for authorisation can be made are not exhaustively enumerated. The complainants are of the view that following the termination of the interference the fate of the information irrelevant for the purposes of the surveillance and the fate of the data related to persons not concerned in the case is not settled. ...

[80] Therefore, within the confines of the complaint the Constitutional Court must examine whether the authorisation by the Minister responsible for justice of secret intelligence gathering for the anti-terrorist organ and the handling of data following the termination of the interference does or does not violate the fundamental rights invoked, namely the right to privacy and the right to informational autonomy....

[92] 3.2. The Constitutional Court has first examined the constitutionality of the authorisation by the Minister responsible for justice. The first phase of secret surveillance is the ordering of the interference. Since in applying section 7/E (3) of the Act on the Police (henceforth: Rtv.) the Minister responsible for justice gives – by authorising the use of the secret intelligence gathering devices and methods listed in

section 56 a)-e) of Nbtv. – consent to a State interference which seriously violates fundamental rights, the process of interference must be regulated under the law, the prescribed norms must be clear, and the process must be subject to external control mechanisms. ...

[94] ... The contested provision of Rtv. authorises the anti-terrorist organ to carry out, in performing certain of its tasks, secret intelligence gathering under the Nbtv. The Rtv. clearly specifies the two tasks for the performance of which secret surveillance under the Nbtv. may be carried out: namely, the performance of the tasks specified in section 7/E (1) a) and ad) and in section 7/E (1) e).

[95] The task specified under section 7/E (1) a) (subsection (ad)) to be performed in the framework of combating terrorism is the prevention, detection and suppression of endeavours to commit an act of terrorism in the territory of Hungary with a view to promoting Hungary's national security interests. Item e) refers back to item d) which allows for the obtaining, analysing, assessing and forwarding of information on a foreign State or originating in a foreign State in so far as the information is necessary for the performance of the task specified there. The tasks specified under item d) are participation in the rescue, return to Hungary and evacuation of Hungarian nationals who have got into trouble due to acts of war or armed conflicts outside the territory of Hungary imminently threatening the lives and limbs of Hungarian nationals or due to terrorist acts or hostage-taking acts, as well as cooperation for such purposes with the member States and institutions of the European Union, the organs of the North Atlantic Treaty Organization, the international organisations concerned by the case and the authorities of the foreign State at issue. These tasks shall be carried out upon a decision to that effect taken by the Minister responsible for law enforcement in agreement with the Minister responsible for foreign affairs.

[96] Section 7/E (3) of Rtv., contested by the complainants, refers to Nbtv. and repeats the Nbtv. rules on secret intelligence gathering (sections 53-60) and the handling of the acquired data [sections 38-52]. Section 7/E (3) of Rtv. provides for the application, *mutatis mutandis*, of the Nbtv. provisions both to the investigation of a complaint about an activity of the anti-terrorist organ, and to the parliamentary control of the anti-terrorist organ and to the investigation of a report alleging unlawful operation on the part of the anti-terrorist organ [section 11 (5), section 14 (1)-(2) and (4) a)-f) and (5), section 15 (3), section 16, section 18 and section 27 (4) of Nbtv.] Moreover, the contested provision clearly provides that the Minister responsible for justice shall be entitled to authorise the use, within the scope of the statutory tasks, of the secret intelligence devices enumerated in an exhaustive list. Therefore section 7/E (3) of Rtv. meets the requirement of being prescribed by law and the requirement of clarity of norms, as it sufficiently specifies the conditions of ordering and the circumstances of executing the measure regulated in the Act.

[97] Thereafter the Constitutional Court has proceeded to examine whether in the given case the authorisation of secret intelligence gathering by the Minister responsible for justice provided sufficient guarantees for the observance of the fundamental rights of the individuals. ...

[102] Secret intelligence gathering for the purposes of national security may only take place under Section 7/E (1) a) ad) or e) of Rtv., that is in order to combat endeavours to commit an act of terrorism in the territory of Hungary and in relation to the protection of Hungarian nationals have got into trouble in a foreign country. ...

[105] The scope of national security-related tasks is much broader than the scope of the tasks related to the investigation of particular crimes as for the purposes of national security the events of real life are examined not for their criminal law

relevance, and those events do not necessarily entail legal consequences. Identifying and combating endeavours aimed at committing acts having relevance from the aspects of securing the sovereignty of the State and of protecting the lawful order of the State may fall outside the sphere of particular criminal offences. Therefore national security-related tasks are not comparable to secret intelligence gathering linked to investigating a crime, which is carried out under section 69 of Rtv. and is subject to authorisation by a court. The prevention and elimination of risks to national security require political decisions, therefore decisions of this type fall in the competence of the executive power. This consideration justifies that general character secret intelligence gathering should be authorised by the Minister responsible for justice.

[106] However, in granting the authorisation the Minister responsible for justice must weigh the interests of national security against the injury done to the fundamental rights. Therefore in addition to assessing the national security interests of the country from a political (home and foreign affairs) aspect, the person granting the authorisation should also strike a fair balance between the interests of national security and fundamental rights. In doing so, it must start from the principle that secret intelligence methods for national security purposes may only be used even by the anti-terrorist organ as a last resort means of detection. Section 53 (2) of Nbtv. clearly provides for the *ultima ratio* nature of secret intelligence methods: the special devices and methods of secret intelligence gathering can only be used where the data needed for the completion of a prescribed task cannot be obtained in any other way, namely by the traditional means of detection. This provision of Nbtv. is intended to serve as a legal guarantee similar to that which the specification in the law of the acts amounting to criminal offences constitutes in the context of secret intelligence gathering linked to the investigation of a particular crime and carried out upon the suspicion of an offence.

[107] ... The request for authorisation must be supported with reasons. The ... grantor of the authorisation shall base his decision on the content of the request: the request shall be granted or, in case of ill-foundedness, rejected. Hence, in case the requesting authority cannot sufficiently justify that the data required for performing its tasks cannot be acquired in any other manner no authorisation for the use of intelligence devices and methods shall be given. ...

[114] As to the ordering and carrying out of the secret intelligence gathering external control is a fundamental guarantee. Control over the activities performed by the anti-terrorist organ under the rules of Nbtv. is exercised by the National Security Committee (henceforth: Committee) of the Parliament ... Upon the Committee's request the Minister of Justice shall provide information on the nature of the authorised information gathering and on the type of the case (section 14(4) b) Nbtv.).

[115] The Committee may acquire information about irregularities related to the operation of the Services (anti-terrorist organ) from, among others, its own inquiries, from citizen complaints or from information from the staff members of the Services. ...

[119] Nbtv. sets one single bar to the Committee's control: the Committee may not learn of information which might endanger the prime importance national security interests in protecting the methods and sources (participating persons) relied on in the case at issue (section 16(1) of Nbtv.) .

[120] The operation of the National Security Services and of the anti-terrorist organ and of the Minister of justice's authorising activity can be controlled, in addition to the Parliament, by the Parliamentary Commissioner for Fundamental Rights as well.

[121] Under section 18 (1) f) of Act no. CXI of 2011 on the Parliamentary Commissioner for Fundamental Rights (henceforth: Ajbt.) law enforcement organs, including the anti-terrorist organ, are authorities that can be examined by the Ombudsman. ... Hence no obstacle exists to an examination by the Ombudsman, the only bar being that – similarly to the control by Parliament – the report made on the examination of the secret intelligence activities of the authorities authorised for using secret intelligence devices and methods may not contain data from which the secret intelligence gathering activities carried out by the organ in the case at issue can be inferred (section 28(3)). The Commissioner for Fundamental Rights may present, in case the conditions specified under section 38 of Ajbt. are met, the cases examined by him to Parliament in an annual report and may, with the exception of motions for amendments, request Parliament to examine a case. ...

[122] On the basis of the above information the Constitutional Court has concluded that Nbtv. allows for the control of the authorisation granting of the Minister of Justice by bodies independent of the executive power. ...

[124] 3.3 In examining the reference in section 7/E (3) of Rtv. the Constitutional Court has observed that section 58 (3) of Nbtv. does not expressly provide for a reasoned decision ...

[127] A necessary element of any judicial decision to be taken on secret intelligence gathering under the Rtv. is an examination of the compliance of the request for authorisation with the statutory requirements. ...

[128] [...] The reference in section 7/E (3) of Rtv. also requires authorisation from the Minister of Justice for national security-related secret intelligence gathering carried out by the anti-terrorist organ, which is part of the Police Service, in order to combat endeavours to commit an act of terrorism in the territory of Hungary or in relation to the protection of Hungarian nationals who have got into trouble in a foreign country. ...

[130] Since Nbtv. does not expressly require the Minister of Justice to issue a reasoned decision, the authoriser is under no obligation to provide reasoning. In the absence of reasoning, however, no posterior understanding, analysis or review of the aspects and reasons giving rise to the decision in a particular case is possible for those who exercise external control.

[131] Though section 58 (3) of Nbtv. prescribes that the authorisation grantor shall base his decision on the content of the request, this content is, per definition, one-sided since in arguing for the necessity of the secret information gathering the request will solely invoke national security interests. The authorisation grantor must strike a fair balance between the interests of national security and fundamental rights enshrined under Article VI (1)-(2) of the Fundamental Law for persons affected by secret intelligence gathering and must ensure, in addition to determining the necessity of the restriction, that the restriction is proportionate. ...

[132] Given that the special nature of secret surveillance excludes the possibility of a remedy, a restriction of the right to privacy and of the right to informational autonomy that is proportionate to the protection of national security will require effective external control already in granting the authorisation for the use of the secret intelligence devices.

[133] The National Security Committee and the Commissioner for Fundamental Rights may only constitute effective external control over the authorisation activity of the Minister of Justice if the Minister's decision authorising the secret surveillance contains sufficiently detailed reasons. The reasons should be of a depth and detail that

enable those who exercise the external control to review the balance struck between the interests of national security and the fundamental rights at issue.

[134] Upon the authorisation granted in section 46 (3) of Abtv., in order to ensure effective external control, the Constitutional Court has laid down as a constitutional requirement ensuring compliance with Article VI (1)-(2) of the Fundamental Law that in applying section 58 (3) of Nbtv. the decision of the Minister responsible for justice ordering secret intelligence gathering must be supported by reasons.

[135] 3.4. Thereafter the Constitutional Court has examined whether the data handling by the anti-terrorist organ following the termination of the secret intelligence gathering violates the right to informational autonomy. The complainants complained that Nbtv., contrary to Rtv., fails to provide for the deletion of such recorded information which is irrelevant for the purposes of the surveillance and of data which are related to persons not concerned by the case. ...

[138] Based on the above considerations the Constitutional Court has established that though Nbtv., contrary to section 73 (3) of Rtv., does not expressly provide for the deletion of such recorded information which is irrelevant for the purposes of the surveillance and of data which are related to persons not concerned by the case, from the joint interpretation of the phrase "obviously unnecessary" in section 50 (2) e) and of section 43 of Nbtv. it clearly follows that any data unnecessary for achieving the aim serving as a legal ground for the data acquisition, in particular the data related to persons not concerned by the case, must be deleted *ex officio*. Therefore the above regulation meets the principle of being purpose-bound and is suitable to prevent storing data acquisition. Moreover, Nbtv. allows for the concerned persons to file a request for the deletion of their personal data, which request can only be rejected by the Chief Director on specific grounds. External control exists over the data processing as well, since the reasons for the rejection of a request must also be sent to the National Data-Protection and Information Freedom Authority [section 48 of Nbtv.].

[139] Therefore the Constitutional Court dismisses, in this respect as well, the complaint alleging non-compliance of the contested provision with the Fundamental Law and seeking the annulment of the contested provision. ..."

III. EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW ("THE VENICE COMMISSION")

21. The Report on the Democratic oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007) (CDL-AD(2007)016-e) contains the following passages:

"81. In the light of the importance and nature of the interests at stake, security intelligence gathering is one of the main areas of national decision-making which a government is most unwilling to submit to national legislative scrutiny and judicial review and, *a fortiori*, to international supervision and control.

82. For a variety of reasons, there can be tension as regards national security policy, not only between the governing party and the political opposition in a State, but also constitutional tension between the executive and the legislative power, tension within a government (especially a coalition government), and tension between political masters and the staff of security intelligence agencies. A large degree of secrecy must accompany national security policy making and operations. However secrecy also has

the effect of increasing the government's control over policy at the expense of the legislative power, and of insulating the former from criticism. This is exacerbated by the fact that nowadays, there is a link between "external" and "internal" threats to the State. Accordingly, security and intelligence information tends to form an indivisible whole. ...

86. It is particularly important, as regards the limited scope of parliamentary and judicial control, to note the special nature of security intelligence. The heart of a security agency is its intelligence files. "Hard" data, purely factual information, is insufficient for a security agency, or for that matter, any police organization. It also needs to gather speculative intelligence in order to determine which people are, or are probably or possibly, threatening national security. This information can be obtained in different ways. A large proportion of non-open source internal security information comes from informants. Like factual information, such "soft intelligence" can, and must if the agency is to do its job properly, be collated to produce a personality profile of a suspect or an analysis of a suspected activity. ...

VII. Internal and Governmental Controls as part of overall accountability systems

130. Internal control of security services is the primary guarantee against abuses of power, when the staff working in the agencies are committed to the democratic values of the State and to respecting human rights. External controls are essentially to buttress the internal controls and periodically ensure these are working properly.

131. Internal controls mean in the first place that the senior management of the agency must exercise efficient control in practice over the lower ranks of the agency.

134. Just as strong internal controls are a precondition for effective executive control over the security agency, a strong executive control over the security agency is a precondition for adequate parliamentary accountability, given that access by parliament to intelligence usually depends on the executive. The same is less true for expert review/authorization systems, to the extent that these have their own access to officials and intelligence material ...

137. In order to provide for impartial verification and assurance for the government that secret agencies are acting according to its policies, effectively and with propriety, a number of countries have devised offices such as Inspectors-General, judicial commissioners or auditors to check on the activities of the security sector and with statutory powers of access to information and staff.

VIII. Parliamentary accountability

150. There are several reasons why parliamentarians should be involved in the oversight of security agencies. Firstly, the ultimate authority and legitimacy of security agencies is derived from legislative approval of their powers, operations and expenditure. Secondly, there is a risk that the agencies may serve narrow political or sectional interests, rather than the State as a whole and protecting the constitutional order, if democratic scrutiny does not extend to them. A stable, politically bi-partisan approach to security may be ensured therefore by proper control, to the benefit of the State and the agencies themselves.

153. From a comparative international perspective, the most frequent arrangement is for parliament to establish a single oversight body for all the major security and intelligence agencies, rather than having multiple oversight bodies for specific agencies.

IX. Judicial Review and Authorization

195. Judicial control over internal security services can take different forms. First, there is prior authorization in a pre-trial phase, and/or post hoc review, of special investigative measures, such as telephone tapping, bugging and video surveillance. This is the normal practice in European States.

204. Nonetheless, there is an obvious advantage of requiring prior judicial authorization for special investigative techniques, namely that the security agency has to go "outside of itself" and convince an independent person of the need for a particular measure. It subordinates security concerns to the law, and as such it serves to institutionalize respect for the law. If it works properly, judicial authorization will have a preventive effect, deterring unmeritorious applications and/or cutting down the duration of a special investigative measure. The Parliamentary Assembly has earlier expressed a clear preference for prior judicial authorization of special investigative measures (depending on the type of measures).

X. Accountability to expert bodies

218. Expert bodies can serve as either a supplement or a replacement for parliamentary bodies or judicial accountability...

219. An expert body allows for greater expertise and time in the oversight of security and intelligence services and avoids the risks of political division and grand-standing to which parliamentary committees can be prone. The body may be full or part time, but even if it is part time, the supervision exerted is likely to be more continuous than that exercised by a parliamentary body, the members of which have many other political interests and responsibilities. The members' tenure can be made longer than the standard electoral period, something which is particularly important as intelligence has, as already mentioned ..., a relatively long "learning curve".

220. Like parliamentary oversight, the mandate of an expert body can be institutional, meaning that it can be established to exercise supervision only over a specific internal security body (this is in contrast to functional review discussed below) ...

222. It is, however, important that the scope of the review is drawn carefully, to avoid disputes as to whether a particular activity falls within the body's mandate and to avoid overlaps with other accountability mechanisms, in particular judicial controls over police powers and Ministerial accountability to parliament.

XI. Complaints mechanisms

241. Clearly it is necessary for individuals who claim to have been adversely affected by the exceptional powers of security and intelligence agencies, such as surveillance or security clearance, to have some avenue for redress. Quite apart from strengthening accountability, complaints may also help to lead to improved performance by the agencies through highlighting administrative failings. The requirements of human rights treaties, and especially the European Convention on Human Rights, with its protections of fair trial, respect for private life and the requirement of an effective remedy must obviously also be borne in mind.

242. Plainly, though, legitimate targets of a security or intelligence agency should not be able to use a complaints system to find out about the agency's work. A complaints system should balance, on the one hand, independence, robustness and fairness, and, on the other hand, sensitivity to security needs. Designing such a system is difficult but not impossible.

243. Individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts. As already mentioned, for a variety of reasons, the capacity of the ordinary courts to serve as an adequate remedy in security fields is limited. The case law of the European Court of Human Rights ... makes it very clear that a remedy must not simply be on paper.

244. An alternative is to allow an investigation and report into a complaint against an agency by an independent official, such as an ombudsman....

245. In these ombudsman-type systems, the emphasis is on an independent official investigating on behalf of the complainant. These independent offices usually exist to deal with an administrative failure by public bodies, rather than a legal error. Their investigations may give less emphasis to the complainant's own participation in the process and to transparency than would be the case with legal proceedings. Typically an investigation of this type will conclude not with a judgment and formal remedies, but with a report, and (if the complaint is upheld) a recommendation for putting matters right and future action...

246. A less common variation is for a State to use a parliamentary or expert oversight body to deal with complaints and grievances of individuals.... There may be a benefit for a parliamentary oversight body in handling complaints brought against security and intelligence agencies since this will give an insight into potential failures – of policy, legality and efficiency. On the other hand, if the oversight body is too closely identified with the agencies it oversees or operates within the ring of secrecy, the complainant may feel that the complaints process is insufficiently independent. In cases where a single body handles complaints and oversight it is best if there are quite distinct legal procedures for these different roles.

247. On the whole it is preferable that the two functions be given to different bodies but that processes are in place so that the oversight body is made aware of the broader implications of individual complaints. This approach is also supported by the ECHR. The requirement in ECHR Article 13 of a mechanism for remedies for alleging violations of Convention rights which is independent from the authorization process means that a State's control system, e.g. for data processing, may pass the test of "accordance with the law" and "necessity in a democratic society" but that the absence of a remedy means that there is nonetheless a violation of the Convention. As already mentioned, the ECtHR has stated that a remedy must be effective in law and fact. It should be noted in particular that the ECtHR has ruled that a data inspection authority which is independent, and which has formal competence in law to award a remedy for the holding of inaccurate, inappropriate etc. security data, but which in fact lacks the expertise to evaluate this data, is not an effective remedy within the meaning of Article 13.

249. In some countries, not only individuals but also members of the services are permitted to bring service-related issues to the attention of an ombudsman or parliamentary oversight body...

250. Another method of handling complaints is through a specialist tribunal."

IV. OTHER RELEVANT INTERNATIONAL TEXTS

22. Several elements of international law, relevant in this context, are outlined in the judgment *Dragojević v. Croatia* (no. 68955/11, §§ 62 to 66, 15 January 2015).

23. In *Digital Rights Ireland v Minister for Communications & Others*, (cases C-293/12 and C-594/12, 8 April 2014), the Court of Justice of the European Union held as follows:

> "26. In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.
>
> 27. Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.
>
> ...
>
> 52. So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 *IPI* EU:C: 2013:715, paragraph 39 and the case-law cited).
>
> ...
>
> 62. In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits."

24. The 2013 Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, contains the following conclusions and recommendations:

"78. Communications techniques and technologies have evolved significantly, changing the way in which communications surveillance is conducted by States. States must therefore update their understandings and regulation of communications surveillance and modify their practices in order to ensure that individuals' human rights are respected and protected.

79. States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.

80. In order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks. To this end, the Special Rapporteur recommends the following:

A. Updating and strengthening laws and legal standards

81. Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.

82. Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.

83. Legal frameworks must ensure that communications surveillance measures:

(a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;

(b) Are strictly and demonstrably necessary to achieve a legitimate aim; and

(c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.

84. States should criminalize illegal surveillance by public or private actors. Such laws must not be used to target whistleblowers or other individuals seeking to expose human rights violations, nor should they hamper the legitimate oversight of government action by citizens.

85. The provision of communications data by the private sector to States should be sufficiently regulated to ensure that individuals' human rights are prioritized at all times. Access to communications data held by domestic corporate actors should only

be sought in circumstances where other available less invasive techniques have been exhausted.

86. The provision of communications data to the State should be monitored by an independent authority, such as a court or oversight mechanism. At the international level, States should enact Mutual Legal Assistance Treaties to regulate access to communications data held by foreign corporate actors.

87. Surveillance techniques and practices that are employed outside of the rule of law must be brought under legislative control. Their extra-legal usage undermines basic principles of democracy and is likely to have harmful political and social effects.

B. Facilitating private, secure and anonymous communications

88. States should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés or mobile telephony.

89. Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys.

90. States should not retain or require the retention of particular information purely for surveillance purposes.

C. Increasing public access to information, understanding and awareness of threats to privacy

91. States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose.

92. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

93. States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance of communications.

94. States should raise public awareness on the uses of new communication technologies in order to support individuals in properly assessing, managing, mitigating and making informed decisions on communications-related risks.

D. Regulating the commercialization of surveillance technology

95. States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection.

96. States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.

97. States must take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and

use of these technologies considering their ability to facilitate systematic human rights violations.

E. Furthering the assessment of relevant international human rights obligations

98. There is a significant need to advance international understanding on the protection of the right to privacy in light of technological advancements. The Human Rights Committee should consider issuing a new General Comment on the right to privacy, to replace General Comment No. 16 (1988).

99. Human rights mechanisms should further assess the obligations of private actors developing and supplying surveillance technologies."

25. The European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs contains the following passages:

The impact of mass surveillance

"...

G. whereas the revelations since June 2013 have caused numerous concerns within the EU as to: ...

- the possibility of these mass surveillance operations being used for reasons other than national security and the fight against terrorism in the strict sense, for example economic and industrial espionage or profiling on political grounds;

- the undermining of press freedom and of communications of members of professions with a confidentiality privilege, including lawyers and doctors;

- the respective roles and degree of involvement of intelligence agencies and private IT and telecom companies;

- the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect and being subject to surveillance;

- the threats to privacy in a digital era and the impact of mass surveillance on citizens and societies;

...

T. whereas fundamental rights, notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination, as enshrined in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy; whereas mass surveillance of human beings is incompatible with these cornerstones;

...

Democratic oversight of intelligence services

BW. whereas intelligence services in democratic societies are given special powers and capabilities to protect fundamental rights, democracy and the rule of law, citizens' rights and the State against internal and external threats, and are subject to democratic

accountability and judicial oversight; whereas they are given special powers and capabilities only to this end; whereas these powers should be used within the legal limits imposed by fundamental rights, democracy and the rule of law and their application should be strictly scrutinised, as otherwise they lose legitimacy and risk undermining democracy;

BX. whereas the fact that a certain level of secrecy is conceded to intelligence services in order to avoid endangering ongoing operations, revealing *modi operandi* or putting at risk the lives of agents, such secrecy cannot override or exclude rules on democratic and judicial scrutiny and examination of their activities, as well as on transparency, notably in relation to the respect of fundamental rights and the rule of law, all of which are cornerstones in a democratic society;

BY. whereas most of the existing national oversight mechanisms and bodies were set up or revamped in the 1990s and have not necessarily been adapted to the rapid political and technological developments over the last decade that have led to increased international intelligence cooperation, also through the large scale exchange of personal data, and often blurring the line between intelligence and law enforcement activities;

BZ. whereas democratic oversight of intelligence activities is still only conducted at national level, despite the increase in exchange of information between EU Member States and between Member States and third countries; whereas there is an increasing gap between the level of international cooperation on the one hand and oversight capacities limited to the national level on the other, which results in insufficient and ineffective democratic scrutiny;

CA. whereas national oversight bodies often do not have full access to intelligence received from a foreign intelligence agency, which can lead to gaps in which international information exchanges can take place without adequate review; whereas this problem is further aggravated by the so-called 'third party rule' or the principle of 'originator control', which has been designed to enable originators to maintain control over the further dissemination of their sensitive information, but is unfortunately often interpreted as applying also to the recipient services' oversight;

CB. whereas private and public transparency reform initiatives are key to ensuring public trust in the activities of intelligence agencies; whereas legal systems should not prevent companies from disclosing to the public information about how they handle all types of government requests and court orders for access to user data, including the possibility of disclosing aggregate information on the number of requests and orders approved and rejected;

Main findings

...

6. Recalls the EU's firm belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection;

7. Considers that data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible existence of other purposes including political and economic espionage, which need to be comprehensively dispelled;

8. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Titles I and VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4(3) of the Treaty on European Union, as well as the principle that Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives';

10. Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing a significant potential for abusive use of the information gathered against political adversaries; emphasises that these mass surveillance activities also entail illegal actions by intelligence services and raise questions regarding the extraterritoriality of national laws;

12. Sees the surveillance programmes as yet another step towards the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence; recalls in this regard the decision of the German Federal Constitutional Court on the prohibition of the use of preventive dragnets ('*präventive Rasterfahndung*') unless there is proof of a concrete danger to other high-ranking legally protected rights, whereby a general threat situation or international tensions do not suffice to justify such measures;

...

14. Points out that the abovementioned concerns are exacerbated by rapid technological and societal developments, since internet and mobile devices are everywhere in modern daily life ('ubiquitous computing') and the business model of most internet companies is based on the processing of personal data; considers that the scale of this problem is unprecedented; notes that this may create a situation where infrastructure for the mass collection and processing of data could be misused in cases of change of political regime; ..."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

26. The applicants complained under Article 8 of the Convention that they could potentially be subjected to measures within the framework of "section 7/E (3) surveillance". They submitted that the legal framework was prone to abuse, notably for want of judicial control.

Article 8 provides as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

27. The Government contested these allegations.

A. Admissibility

1. The parties' submissions

28. The Government did not formally contest the applicants' potential victim status within the meaning of the Court's jurisprudence, under which the mere existence of a piece of legislation allowing for the use of secret intelligence devices served as a ground for victim status, even if no such device had ever been used against an applicant. However, the Government disputed the applicants' allegations that – as staff members of a watchdog organisation – they were affected more directly by the possibility of being subjected to secret surveillance than others.

29. Moreover, the Government submitted that in their constitutional complaint the applicants had not complained about the presence or absence of guarantees in the entire process of secret intelligence gathering. They had only complained about the authorisation by the Minister of Justice of the interference and the data handling following the termination of the interference. The Government emphasised that in respect of any further complaints that the applicants might have in relation to other phases of the process, they had failed to exhaust the available domestic remedies.

30. Regarding victim status, the applicants emphasised that the lack of meaningful external control over the use of covert surveillance had put individuals' privacy in danger as nothing prevented the political power from using this prerogative arbitrarily. Their watchdog activity might not serve as a ground for secret intelligence gathering. Nevertheless, their statement - according to which they, as staff members of watchdog organisations voicing criticism against the Government, felt more frustrated and worried about being subjected to secret surveillance than average citizens probably did – could not be regarded as fear based on completely unfounded assumptions, especially if considering some of the Government's recent measures as being directed against civil organisations.

31. Concerning exhaustion of domestic remedies, the applicants did not dispute that their constitutional complaint had been focused on the system of authorisation, since only the safeguards built into this phase were able to

provide adequate protection to right to privacy. This meant that guarantees related to later procedural phases were unable to counterbalance the detriment caused to the right to privacy if there was no control mechanism built into the process of authorisation of secret surveillance that was able to impede legally unjustifiable interventions into the private sphere. However, the question as to whether this assertion was correct might only be assessed considering the procedure as a whole. The Government's suggestion that the Court should refrain from the assessment of procedural phases beyond the authorisation phase was pointless and practically not feasible. Moreover, the applicants emphasised that the complaint lodged with the Constitutional Court and the complaint submitted to the Court did not completely correspond to each other in terms of the arguments forwarded, and that therefore the Court should not refrain, purely relying on the principle of subsidiarity, from examining the question as to whether the other guarantees provided in the procedure ensured adequate protection.

2. The Court's assessment

32. As to the applicants' victim status, the Court has consistently held in its case-law that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention (see, *inter alia*, *Klass and Others v. Germany*, 6 September 1978, § 33, Series A no. 28; *N.C. v. Italy* [GC], no. 24952/94, § 56, ECHR 2002-X; and *Krone Verlag GmbH & Co. KG v. Austria* (no. 4), no. 72331/01, § 26, 9 November 2006).

33. However, in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him. The Court's approach to assessing whether there has been an interference in cases raising a complaint about the legislation allowing secret surveillance measures was set out in its *Klass and Others* judgment (cited above, §§ 34 and 36) as follows:

> "34. ... the effectiveness (*l'effet utile*) of the Convention implies in such circumstances some possibility of having access to the Commission. If this were not so, the efficiency of the Convention's enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious.
>
> The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case

according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures.

...

36. The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8, or even to be deprived of the right granted by that Article, without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions. ...

The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25, since otherwise Article 8 runs the risk of being nullified."

34. Following *Klass and Others* (cited above) and *Malone v. the United Kingdom* (2 August 1984, § 64, Series A no. 82), the former Commission, in a number of cases against the United Kingdom in which the applicants alleged actual interception of their communications, emphasised that the test in *Klass and Others* could not be interpreted so broadly as to encompass every person in the United Kingdom who feared that the security services may have conducted surveillance of him. Accordingly, the Commission required applicants to demonstrate that there was a "reasonable likelihood" that the measures had been applied to them (see, for example, *Esbester v. the United Kingdom*, no. 18601/91, Commission decision of 2 April 1993; *Redgrave v. the United Kingdom*, no. 20271/92, Commission decision of 1 September 1993; and *Matthews v. the United Kingdom*, no. 28576/95, Commission decision of 16 October 1996); subsequently, the Court applied a similar approach (see *Halford v. the United Kingdom*, 25 June 1997, §§ 56 to 57, *Reports of Judgments and Decisions* 1997-III).

35. More pertinently with regard to the present application, in other cases which concerned complaints about the legislation and practice permitting secret surveillance measures, the Court has reiterated the *Klass and Others* approach on a number of occasions (see, *inter alia*, *Weber and Saravia* (dec.), no. 54934/00, § 78, ECHR 2006 XI; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 58 to 60, 28 June 2007; *Iliya Stefanov v. Bulgaria*, no. 65755/01, § 49, 22 May 2008; *Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 56 to 57, 1 July 2008; and *Iordachi and Others v. Moldova*, no. 25198/02, §§ 30 to 35, 10 February 2009).

36. In the case of *Kennedy v. the United Kingdom* (no. 26839/05, § 124, 18 May 2010) the Court held that in order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court

must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by the Court.

Most recently, the Court adopted, in *Roman Zakharov v. Russia* ([GC], no. 47143/06, §§ 170-172, 4 December 2015), a harmonised approach based on *Kennedy*, according to which firstly the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affect all users of communication services by instituting a system where any person can have his or her communications intercepted; and secondly the Court will take into account the availability or remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies.

37. The Court observes that the present applicants complained of an interference with their homes, communications and privacy on the basis of the very existence of the law permitting secret surveillance and the lack of adequate safeguards, admitting that their personal or professional situations were not of the kind that might normally attract the application of surveillance measures. They nevertheless thought they were at particular risk of having their communications intercepted as a result of their employment with civil-society organisations criticising the Government.

38. The Court observes that affiliation with a civil-society organisation does not fall within the grounds listed in section 7/E (1) point (a) sub-point (*ad*) and point (e) of the Police Act, which concern in essence terrorist threats and rescue operations to the benefit of Hungarian citizens in dangerous situations abroad. Nevertheless, it appears that under these provisions any person within Hungary may have his communications intercepted if interception is deemed necessary on one of the grounds enumerated in the law (see paragraph 16 above). The Court considers that it cannot be excluded that the applicants are at risk of being subjected to such measures should the authorities perceive that to do so might be of use to pre-empt or avert a threat foreseen by the legislation – especially since the law contains the notion of "persons concerned identified ... as a range of persons" which might include indeed any person.

The Court also notes that, by examining their constitutional complaint on the merits, the Constitutional Court implicitly acknowledged the applicants' being personally affected by the legislation in question for the purposes of section 26(1) of the Act on the Constitutional Court (see paragraph 19 above).

It is of importance at this juncture to note that they are staff members of a watchdog organisation, whose activities have previously been found similar, in some ways, to those of journalists (see *Társaság a Szabadságjogokért v. Hungary*, no. 37374/05, § 36, 14 April 2009). The Court accepts the applicants' suggestion that any fear of being subjected to secret surveillance might have an impact on such activities (see, *mutatis mutandis*, *Nagla v. Latvia*, no. 73469/10, § 82, 16 July 2013). In any case, whether or not the applicants belong to a targeted group, the Court considers that the legislation directly affects all users of communication systems and all homes.

39. Considering in addition that the domestic law does not appear to provide any possibility for an individual who alleges interception of his or her communications to lodge a complaint with an independent body, the Court is of the view that the applicants can claim to be victims of a violation of their rights under the Convention, within the meaning of Article 34 of the Convention.

40. Concerning the exhaustion of domestic remedies, the Court is satisfied that the applicants brought to the attention of the national authorities, in the instant case the Constitutional Court, the essence of their grievance, that is, the alleged insufficiency of guarantees in the rules governing "section 7/E (3) surveillance". While noting the Government's objection according to which this constitutional complaint was focused on but a few central issues, the Court considers that, because of the nature of the problem, the system of guarantees preceding the measures, prevailing during their application and following it is a complex set of arrangements which must be assessed in its entirety (see *Klass and Others*, cited above, §§ 39 to 60). Consequently – and assuming that the procedure before the Constitutional Court was at all an effective remedy to exhaust in the circumstances – the fact that the applicants' constitutional complaint did not encompass all possible issues but highlighted a few cannot be held against them so as to enable the rejection of their complaints on account of non-exhaustion of domestic remedies, in so far as their representations made to the Court on these issues can be seen as supplementing the ones submitted to the Constitutional Court (see, *mutatis mutandis*, *Gustafsson v. Sweden*, 25 April 1996, § 51, *Reports* 1996-II).

41. Moreover, the Court concludes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. No other ground for declaring it inadmissible has been established. It must therefore be declared admissible.

B. Merits

1. Arguments of the parties

(a) The Government

42. With regard to the necessity of judicial authorisation in the context of Article 8, the Government referred to the Venice Commission's Report on the Democratic Oversight of the Security Services (CDL-AD(2007)016, adopted at the Venice Commission's 71st Plenary Session, Venice, 1-2 June 2007). Relying on several observations made in this report, the Government submitted that the domestic courts were not suitable to determine the necessity of secret intelligence gathering for national security purposes due to the nature of the data to be assessed, to the inherent subjectivity of the risk assessment, to the political nature of the notion of national security and to the wide margin of appreciation afforded in this field to the Government.

43. In the Government's view, it was an inherent feature of a judicial decision that the judge examines the compliance of the proposed decision with the rules of positive law or with rules that could be inferred from positive law. In the field of authorising national security-purposed secret intelligence gathering no positive law specifying any exact criteria providing grounds for judicial decisions existed or could be created. The reason for that was that, in authorising national security secret intelligence gathering, the decision, for which the decision-maker bore political responsibility, was to be taken by assessing the country's security interests and by taking into account home and foreign political aspects. Consequently, the Minister of Justice – bearing political responsibility - was a person more qualified than judges to make such decisions. In any case, experience showed that judicial review in this field was not more apt than governmental supervision.

44. Moreover, the Government reiterated that the national security related authorisation activity of the Minister of Justice had always been controlled by the Parliamentary Committee for National Security and by the Data Protection Ombudsman and there were no signs indicating that the authorisation mechanism was formal or arbitrary.

45. Finally, the Government argued – relying on the observations made by the Court in *Klass and Others* (cited above), in *Goranova-Karaeneva v. Bulgaria* (no. 12739/05, 8 March 2011) and in *Golder v. the United Kingdom* (21 February 1975, Series A no. 18) – that the complaint related to the lack of an effective legal remedy under Article 13 was manifestly ill-founded.

(b) The applicants

46. Replying to the arguments based on the Venice Commission's Report, the applicants stressed that because ordinary courts were, in

practice, frequently confronted with difficulties in dealing with the large discretion afforded to the Government in this area, as observed by the Venice Commission, it could not be concluded that judicial control resulted in a less adequate control of secret surveillance for national security purposes. The actual conclusion of the Report was that only a complex arrangement of guarantees designed to involve judges in the control of security services could ensure the adequate protection of individuals. As pointed out in the Venice Convention's Report, "[i]n order for judicial control to be effective, the judges must be independent and possess the necessary expertise".

47. The applicants also emphasised that the preconditions for the use of special secret surveillance instruments and methods of intelligence information gathering were not precisely defined in the law and this might also lead to arbitrary decision-making in the absence of judicial control. In this connection the applicants referred to the Court's case-law, arguing that restrictions on the right to privacy by means of secret surveillance might only be in line with the Convention if the restriction was properly defined by the law (cf. *Malone*, cited above).

48. The applicants further argued that the Data Protection Ombudsman and the Parliamentary Committee for National Security were not a substitute for the judicial control in the authorisation phase since they constituted oversight, rather than remedial, mechanisms and these had only general consequences not affecting the concrete case. Upon queries addressed to these two organs, the applicants found that none of them had ever dealt with a case on surveillance of citizens. These potential control mechanisms were thus not effective.

(c) The third parties

(i) Center for Democracy & Technology (CDT)

49. The CDT drew the Court's attention to the States' advanced present-day capabilities for sophisticated and invasive surveillance, as well as to their ability to build a detailed profile of any individual's activities and relationships using intercepted data. It mentioned the vast amount of information that could be retrieved from a physically seized computer or other personal electronic device. It further emphasised the development of the possibilities to intercept communication and metadata, such as contacts and location information, remotely, by tapping Internet or telephone networks. In addition to mass surveillance and the sophisticated analysis of the intercepted data, States were also able to conduct targeted surveillance of specific individuals by installing remotely malicious software on their devices, even enabling secret surveillance agencies to record keystrokes, sounds, photos or videos, unbeknown to the owner.

50. According to the CDT, in the light of such surveillance capabilities, Article 8 required judicial oversight over all secret surveillance programmes conducted for the purpose of national security. Regarding those exceptional cases where judicial oversight was impossible, the CDT invited the Court to provide clear guidance to Contracting Parties and applicants by adopting a set of specific criteria for determining whether a non-judicial oversight process was sufficient to prevent the abuse of Article 8 rights – although the CDT maintained that Article 8 nevertheless required judicial control as the last resort. Finally, the CDT concluded that anyone within the jurisdiction of a Contracting Party who had a credible claim to have been the victim of an Article 8 violation arising from a secret national security surveillance programme must have access to a remedy that was effective in the sense that the remedial body was obliged to conduct an investigation into the complaint, and was both empowered and obligated to provide effective redress for the violation.

(ii) Privacy International

51. Privacy International reviewed the relevant jurisprudence, both of the Court and national courts in Europe, Canada and the United Sates, highlighting recent decisions affirming that surveillance measures, including mere access to data retained by communications service providers, must be subject to judicial control or dependent upon the issuance of a judicial warrant. Moreover, Privacy International overviewed the international human rights standards relevant to the question of judicial control of surveillance, referring - among other things - to United Nations announcements and to the International Principles on the Application of Human Rights to Communications Surveillance which all include the need for judicial control of surveillance and for the right to an effective remedy.

2. The Court's assessment

52. It is not in dispute between the parties that the measures which the TEK is entitled to apply under section 56 of the National Security Act (see paragraph 17 above), that is, to search and keep under surveillance the applicants' homes secretly, to check their postal mail and parcels, to monitor their electronic communications and computer data transmissions and to make recordings of any data acquired through these methods can be examined from the perspective of the notions of "private life", "home" and "correspondence", guaranteed under Article 8 of the Convention. The Court sees no reason to hold otherwise (see *Klass and Others*, cited above, § 41).

53. In the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right

to respect for private and family life and for correspondence (see *Klass and Others*, cited above, § 41). Given the technological advances since the *Klass and Others* case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely (see *Copland v. the United Kingdom*, no. 62617/00, § 41, ECHR 2007-I).

54. Any interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim. This provision, "since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions" (see *Klass and Others*, cited above, § 42).

55. The Court finds that the aim of the interference in question is to safeguard national security and/or to prevent disorder or crime in pursuance of Article 8 § 2. This has not been in dispute between the parties. On the other hand, it has to be ascertained whether the means provided under the impugned legislation for the achievement of the above-mentioned aim remain in all respects within the bounds of what is necessary in a democratic society (see *Klass and Others*, cited above, § 46).

56. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed (see *Huvig v. France*, 24 April 1990, § 34, Series A no. 176-B; *Amann* v. *Switzerland* [GC], no. 27798/95, §§ 56-58, ECHR 2000-11; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, *Reports* 1998-V; *Prado Bugallo v. Spain,* no. 58496/00, § 30, 18 February 2003; *Weber and Saravia,* cited above, § 95; *Association for European Integration,* cited above, § 76; and *Roman Zakharov*, cited above, § 231).

57. When balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national

security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society" (see *Klass and Others,* cited above, §§ 49, 50 and 59; *Weber and Saravia,* cited above, §106; *Kvasnica* v. *Slovakia,* no. 72094/01, § 80, 9 June 2009; *Kennedy,* cited above, §§ 153 and 154; and *Roman Zakharov*, cited above, § 232).

58. The Court has found an interference under Article 8 § 1 in respect of the applicants' general complaint about the rules of "section 7/E (3) surveillance" and not in respect of any actual interception activity allegedly taking place. Accordingly, in its examination of the justification for the interference under Article 8 § 2, the Court is required to examine this legislation itself and the safeguards built into the system allowing for secret surveillance, rather than the proportionality of any specific measures taken in respect of the applicants. In the circumstances, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with in respect of the "section 7/E (3) surveillance" regime and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (see *Kvasnica*, cited above, § 84).

59. The expression "in accordance with the law" in Article 8 § 2 requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him (see, among other authorities, *Kruslin v. France*, 24 April 1990, § 27, Series A no. 176-A; *Huvig*, cited above, § 26; *Lambert v. France*, 24 August 1998, § 23, *Reports* 1998-V; *Perry v. the United Kingdom*, no. 63737/00, § 45, ECHR 2003-IX (extracts); *Dumitru Popescu v. Romania (no. 2)*, no. 71525/01, § 61, 26 April 2007; *Association for European Integration*, cited above, § 71; and *Liberty*, cited above, § 59). The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse (see *Roman Zakharov*, cited above, § 236).

60. It is not in dispute that the interference in question had a legal basis. The relevant rules are contained in statute law, that is, in the Police Act and

the National Security Act. Their accessibility has not been called into question.

61. The applicants, however, contended that this law was not sufficiently detailed and precise to meet the "foreseeability" requirement of Article 8 § 2, as it did not provide for sufficient guarantees against abuse and arbitrariness.

62. The reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. 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 (see *Roman Zakharov*, cited above, § 229).

63. In the present case, two situations may entail secret surveillance, namely, the prevention, tracking and repelling of terrorist acts in Hungary (section 7/E (1) a) (*ad*) of the Police Act) and the gathering of intelligence necessary for rescuing Hungarian citizens in distress abroad (section 7/E (1) e), see in paragraph 16 above).

The applicants criticised these rules as being insufficiently clear.

64. The Court is not wholly persuaded by this argument, recalling that the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague (see *Kokkinakis v. Greece*, 25 May 1993, § 40, Series A no. 260-A). It is satisfied that even in the field of secret surveillance, where foreseeability is of particular concern, the danger of terrorist acts and the needs of rescue operations are both notions sufficiently clear so as to meet the requirements of lawfulness. For the Court, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations. The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication (compare and contrast *Iordachi and Others*, cited above, § 46). For the Court, nothing indicates in the text of the relevant legislation that the notion of "terrorist acts", as used in section 7/E (1) a) (*ad*) of the Police Act, does not correspond to the crime of the same denomination contained in the Criminal Code (see paragraph 16 above).

65. However, in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 247).

66. The Court notes that under "section 7/E (3) surveillance", it is possible for virtually any person in Hungary to be subjected to secret surveillance. The legislation does not describe the categories of persons who, in practice, may have their communications intercepted. In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the underlying situations be clearly defined. The relevant circumstances which can give rise to interception, discussed in the preceding paragraphs, give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted. Under the relevant Hungarian law, the proposal submitted to the responsible government minister must specify, either by name or as a range of persons, the person or persons as the interception subjects and/or any other relevant information capable of identifying them as well as the premises in respect of which the permission is sought (section 57 (2) of the National Security Act, see paragraph 17 above).

67. It is of serious concern, however, that the notion of "persons concerned identified ... as a range of persons" might include indeed any person and be interpreted as paving the way for the unlimited surveillance of a large number of citizens. The Court notes the absence of any clarification in domestic legislation as to how this notion is to be applied in practice (see, *mutatis mutandis*, *Roman Zakharov*, cited above, § 245). For the Court, the category is overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons "concerned" and the prevention of any terrorist threat – let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity (see in paragraphs 72 and 73 below) with regard to the aims pursued and the means employed – although such an analysis appears to be warranted by section 53 (2) of the National Security Act, according to which "secret intelligence gathering [may only be applied] if the intelligence needed ... cannot be obtained in any other way".

68. For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of

communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen (see the CDT's submissions on this point in paragraphs 49-50 above), especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information (see paragraphs 23 and 24 above).

69. The Court recalls that in *Kennedy*, the impugned legislation did not allow for "indiscriminate capturing of vast amounts of communications" (see *Kennedy*, cited above, § 160) which was one of the elements enabling it not to find a violation of Article 8. However, in the present case, the Court considers that, in the absence of specific rules to that effect or any submissions to the contrary, it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern.

70. The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile (see the CDT's submissions on this in paragraph 49 above) of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament (see paragraphs 23 and 25 above). This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices. However, it is not warranted to embark on this matter in the present case, since the

Hungarian system of safeguards appears to fall short even of the previously existing principles.

71. Moreover, under section 57 (2) b), in the motion requesting permission from the Minister, the director must substantiate the necessity for the secret intelligence gathering (see paragraph 17 above). However, reading the relevant provisions jointly, the Court is not reassured that an adequate analysis of the aims pursued and the means applied in performing the national security tasks is possible or guaranteed. Indeed, the mere requirement for the authorities to give reasons for the request, arguing for the necessity of secret surveillance, falls short of an assessment of strict necessity (see in paragraphs 72 and 73 below). There is no legal safeguard requiring TEK to produce supportive materials or, in particular, a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure - and this on the basis of an individual suspicion regarding the target person (see *Roman Zakharov*, cited above, §§ 259 and 261). For the Court, only such information would allow the authorising authority to perform an appropriate proportionality test.

72. Quite apart from what transpires from section 53(2) of the National Security Act, the Court recalls at this point that in *Klass and Others* it held that "powers of secret surveillance of citizens ... are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions" (see *Klass and Others*, cited above, § 42, quoted in paragraph 54 above). Admittedly, the expression "strictly necessary" represents at first glance a test different from the one prescribed by the wording of paragraph 2 of Article 8, that is, "necessary in a democratic society".

73. However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity (see paragraphs 23 and 24 above) – an approach it considers convenient to endorse. Moreover, particularly in this context the Court notes the absence of prior judicial authorisation for interceptions, the importance

of which will be examined below in paragraphs 75 *et seq*. This safeguard would serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "persons concerned identified ... as a range of persons" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case (see, *mutatis mutandis*, *Roman Zakharov*, cited above, § 249). It is only in this way that the need for safeguards to ensure that emergency measures are used sparingly and only in duly justified cases can be satisfied (see *Roman Zakharov*, cited above, § 266).

74. Furthermore, in respect of the duration of any surveillance, the National Security Act stipulates, first, the period after which a surveillance permission will expire (that is, after a maximum of 90 days, as per section 58 (4) of the National Security Act) and, second, the conditions under which a renewal is possible. Permissions can be renewed for another 90 days; and the government minister in charge must authorise any such renewal upon a reasoned proposal from the service involved (see paragraph 17 above). Section 60 stipulates that the permission must be cancelled if it is no longer necessary, if the continued surveillance has no prospect of producing results, if its time-limit has expired or if it turns out to be in breach of the law for any reason. The Court cannot overlook, however, that it is not clear from the wording of the law – especially in the absence of judicial interpretation – if such a renewal of the surveillance warrant is possible only once or repeatedly, which is another element prone to abuse.

75. A central issue common to both the stage of authorisation of surveillance measures and the one of their application is the absence of judicial supervision. The measures are authorised by the Minister in charge of justice upon a proposal from the executives of the relevant security services, that is, of the TEK which, for its part, is a dedicated tactical department within the police force, subordinated to the Ministry of Home Affairs, with extensive prerogatives to apply force in combating terrorism (see section 1(2) subsection 15 of the Police Act quoted in paragraph 16 above). For the Court, this supervision, eminently political (as observed by the Constitutional Court, see point 105 of the decision quoted in paragraph 20 above) but carried out by the Minister of Justice who appears to be formally independent of both the TEK and of the Minister of Home Affairs – is inherently incapable of ensuring the requisite assessment of strict necessity with regard to the aims and the means at stake. In particular, although the security services are required, in their applications to the Minister for warrants, to outline the necessity as such of secret information gathering, this procedure does not guarantee that an assessment of strict necessity is carried out, notably in terms of the range of persons and the premises concerned (see section 57 (2) of the National Security Act quoted in paragraph 17 above).

76. The Court notes the Government's argument according to which a government minister is better positioned than a judge to authorise or supervise measures of secret surveillance. Although this consideration might be arguable from an operational standpoint, the Court is not convinced of the same when it comes to an analysis of the aims and means in terms of strict necessity. In any case, it transpires from the parties' submissions that anti-terrorism surveillance measures in Hungary have never been subjected to judicial control, for which reason it is not possible to pass judgement on its advantages or drawbacks. The Court finds therefore the Government's argument on this point unpersuasive (see, *a contrario*, *Roman Zakharov*, cited above, § 259).

77. As regards the authority competent to authorise the surveillance, authorising of telephone tapping by a non-judicial authority may be compatible with the Convention (see, for example, *Klass and Others,* cited above, § 51; *Weber and Saravia,* cited above, § 115; and *Kennedy,* cited above, § 31), provided that that authority is sufficiently independent from the executive (see *Roman Zakharov*, cited above, § 258). However, the political nature of the authorisation and supervision increases the risk of abusive measures. The Court recalls that the rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see *Klass and Others*, cited above, §§ 55 and 56). The Court recalls that in *Dumitru Popescu* (cited above, §§ 70-73) it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see *Klass and Others*, cited above, §§ 42 and 55). The *ex ante* authorisation of such a measure is not an absolute requirement *per se*, because where there is extensive *post factum* judicial oversight, this may counterbalance the shortcomings of the authorisation (see *Kennedy*, cited above, § 167). Indeed, in certain respects and for certain circumstances, the Court has found already that *ex ante* (quasi-)judicial authorisation is necessary, for example in regard to secret surveillance measures targeting the media. In that connection the Court held that a *post factum* review cannot restore the confidentiality of journalistic sources once it is destroyed (see *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, § 101,

22 November 2012; for other circumstances necessitating *ex ante* authorisation see *Kopp v. Switzerland*, 25 March 1998, *Reports* 1998 II).

For the Court, supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees.

78. The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures.

79. It is in this context that the external, preferably judicial, *a posteriori* control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance (see also *Klass and Others*, cited above, §§ 56, 70 and 71; *Dumitru Popescu*, cited above, § 77; and *Kennedy*, cited above, §§ 184-191), by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained. The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks. The Court notes the lack of such a control mechanism in Hungary.

80. The Court concedes that by the nature of contemporary terrorist threats there can be situations of emergency in which the mandatory application of judicial authorisation is not feasible, would be counterproductive for lack of special knowledge or would simply amount to wasting precious time. This is especially true in the present-day upheaval caused by terrorist attacks experienced throughout the world and in Europe, all too often involving important losses of life, producing numerous casualties and significant material damage, which inevitably disseminate a feeling of insecurity amongst citizens. The observations made on this point by the Court in *Klass and Others* are equally valid in the circumstances of the present case: "[d]emocratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime" (cited above, § 48).

81. Furthermore, where situations of extreme urgency are concerned, the law contains a provision under which the director of the service may himself authorise secret surveillance measures for a maximum of 72 hours (see sections 58 and 59 of the National Security Act quoted in paragraph 17 above). For the Court, this exceptional power should be sufficient to address any situations in which external, judicial control would run the risk of losing precious time. Such measures must however be subject to a *post factum* review, which is required, as a rule, in cases where the surveillance was authorised *ex ante* by a non-judicial authority.

82. The Court notes at this juncture the liability of the executive to give account, in general terms rather than concerning any individual cases, of such operations to a parliamentary committee. However, it cannot identify any provisions in Hungarian legislation permitting a remedy granted by this procedure during the application of measures of secret surveillance to those who are subjected to secret surveillance but, by necessity, are kept unaware thereof. The Minister is under an obligation to present a general report, at least twice a year, to the responsible parliamentary committee about the functioning of national security services, which report, however, does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny (see *Roman Zakharov*, cited above, § 283). The committee is entitled, of its own motion, to request information from the Minister and the directors of the services about the activities of the national security services. However, the Court is not persuaded that this scrutiny 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 documents. The scope of their supervision is therefore limited (see, *mutatis mutandis*, *Roman Zakharov*, cited above, § 281).

83. Moreover, the complaint procedure outlined in section 11(5) of the National Security Act seems to be of little relevance, since citizens subjected to secret surveillance will not take cognisance of the measures applied. In regard to the latter point, the Court shares the view of the Venice Commission according to which "individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts." (see point 243 of the Report, quoted in paragraph 21 above). A complaint under section 11(5) of the National Security Act will be investigated by the Minister of Home Affairs, who does not appear to be sufficiently independent (see *Association for European Integration*, cited above, § 87; and *Roman Zakharov*, cited above, § 278).

84. The Court further notes the evidence furnished by the applicants according to which the Commissioner for Fundamental Rights has never so far enquired into the question of secret surveillance (see paragraph 18 above).

85. In any event, the Court recalls that in *Klass and Others* a combination of oversight mechanisms, short of formal judicial control, was found acceptable in particular because of "an initial control effected by an official qualified for judicial office" (cited above, § 56). However, the Hungarian scheme of authorisation does not involve any such official. The Hungarian Commissioner for Fundamental Rights has not been demonstrated to be a person who necessarily holds or has held a judicial office (see, *a contrario*, *Kennedy*, cited above, § 57).

86. Moreover, the Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned (see *Weber and Saravia*, cited above, §135; *Roman Zakharov*, cited above, § 287). In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates that the legislation falls short of securing adequate safeguards.

87. It should be added that although the Constitutional Court held that various provisions in the domestic law read in conjunction secured sufficient safeguards for data storage, processing and deletion, special reference was made to the importance of individual complaints made in this context (see point 138 of the decision, quoted in paragraph 20 above). For the Court, the latter procedure is hardly conceivable, since once more it transpires from the legislation that the persons concerned will not be notified of the application of secret surveillance to them.

88. Lastly, the Court notes that is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples (see *Roman Zakharov*, cited above, § 284). However, the Government were not able to do so in the instant case.

89. In total sum, the Court is not convinced that the Hungarian legislation on "section 7/E (3) surveillance" provides safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures.

Given that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and

without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention.

II. ALLEGED VIOLATIONS OF ARTICLE 6 AND ARTICLE 13 READ IN CONJUNCTION WITH ARTICLE 8 OF THE CONVENTION

90. The applicants further complained that their exposure to secret surveillance measures without judicial control or remedy amounted to a violation of their rights under Article 6 as well as Article 13 read in conjunction with Article 8 of the Convention.

91. The Government contested that argument.

92. The Court notes that these complaints are linked to the one examined above and must therefore likewise be declared admissible.

93. The Court reiterates that Article 13 cannot be interpreted as requiring a remedy against the state of domestic law (see *Ostrovar v. Moldova*, no. 35207/03, § 113, 13 September 2005; *Iordachi*, cited above, § 56). In these circumstances, the Court finds no breach of Article 13 of the Convention taken together with Article 8.

94. Moreover, having regard to the finding relating to Article 8 (see paragraph 89 above), the Court considers that it is not necessary to examine whether, in this case, there has been a violation of Articles 6 of the Convention.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

95. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

96. Each applicant claimed 10,000 euros (EUR) in respect of non-pecuniary damage.

97. The Government found the claim excessive.

98. The Court considers that in the circumstances of the present case the finding of a violation of Article 8 constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained.

B. Costs and expenses

99. The applicants also claimed, jointly, EUR 7,500 for the costs and expenses incurred before the Constitutional Court and the Court in Strasbourg. This corresponds to altogether 50 hours of legal work billable by their lawyer at an hourly rate of EUR.

100. The Government contested this claim.

101. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 4,000 covering costs under all heads.

C. Default interest

102. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 8 of the Convention;

3. *Holds* that there has been no violation of Article 13 read in conjunction with Article 8 of the Convention;

4. *Holds* that there is no need to examine the complaint under Article 6 of the Convention;

5. *Holds* that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicants;

6. *Holds*

   (a) that the respondent State is to pay the applicants, jointly, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 4,000 (four thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses, to be converted into the currency of the respondent State at the rate applicable at the date of settlement;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

7. *Dismisses* the remainder of the applicants' claim for just satisfaction.

Done in English, and notified in writing on 12 January 2016, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Fatoş Aracı	V. De Gaetano
Deputy Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Pinto de Albuquerque is annexed to this judgment.

V.D.G.
F.A.

CONCURRING OPINION OF JUDGE PINTO DE ALBUQUERQUE

1. The chamber is unanimous in finding a violation of Article 8, but I am not satisfied with the reasoning of the judgment. In two crucial issues, the Chamber departs deliberately from the Grand Chamber judgment delivered in the very recent *Roman Zakharov v. Russia* case[1], which set the European standard on mass surveillance for intelligence and national security purposes. The two points of confrontation between the Chamber's reasoning and the one provided by the Grand Chamber relate to the question of the necessity test for determining covert surveillance operations and the degree of suspicion of involvement in the offences or activities surveilled.

2. I cannot agree with the Chamber's posture, for two imperative reasons: firstly, because I already took a different position on these issues in my separate opinion joined to the judgment delivered in the *Draksas v. Lithuania* case on phone tapping and other communication interception as covert surveillance and intelligence gathering measures[2], which should not be confused with special investigation techniques in the criminal law field[3]; secondly, my opinion in *Draksas* was confirmed, in substance, by the Grand Chamber in the above mentioned Russian case. Hence, nothing could justify my defiance to the Grand Chamber's findings in *Roman Zakharov*. That is why, in the following opinion, I will seek to defend the Grand Chamber's findings and deconstruct the present judgment's reasoning where it departed from them.

Mass surveillance for the purpose of national security in international law

3. Since the disclosure of mass surveillance practices in June 2013 by the former United States National Security Agency (US NSA) contractor Mr. Edward Snowden, the discussion on the issue of protection of privacy has regained a new impetus in the United Nations. In a chillingly accurate forecast, the Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, of 17 April 2013, analyzed the implications of States'

---

[1] *Roman Zhakarov v. Russia (GC)*, no. 47143/06, 4 December 2015.
[2] *Draksas v. Lithuania*, no. 36662/04, 31 July 2012.
[3] See my opinion joined in the case of *Lagutin and Others v. Russia*, nos. 6228/09, 19123/09, 19678/07, 52340/08 and 7451/09, 24 April 2014. This case related to law enforcement and criminal investigations, whose standards differ from those of secret surveillance for national security purposes. It should be noted that the Chamber often confuses these standards (see for example paragraphs 22 and 56 of the judgment citing elements of international law and Court cases relevant for criminal investigation purposes).

surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression[4]. Immediately after the Snowden revelations, on 21 June 2013, the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights considered it necessary to highlight a series of international legal principles on the issue and published a "Joint Declaration on surveillance programs and their impact on freedom of expression"[5]. On 26 September 2013, the 35th International Conference of Data Protection and Privacy Commissioners adopted a "Resolution on anchoring data protection and the protection of privacy in international law". The Commissioners resolved to call upon governments to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No. 16 to the Covenant.

4. On 18 December 2013, the United Nations General Assembly adopted Resolution 68/167, on "the Right to Privacy in the Digital Age"[6], which

---

[4] A/HRC/23/40. The Rapporteur advocated judicial supervision of State surveillance of communications, the right of the surveilled person to be notified once the operation has been completed and the right to seek redress (paras. 81 and 82). Prior to that report, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism put forward the "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight", 17 May 2010 (A/HRC/14/46). Important documents of the civil society were also published on this topic. The "International Principles on the Application of Human Rights to Communications Surveillance", endorsed by almost 400 non-governmental and human rights organisations, were launched in May 2014. The Open Society Justice Initiative published the "Global Principles on National Security and the Right to Information (Tshwane Principles)", on 12 June 2013, which were drafted by 22 organizations and academic centers, following the "Johannesburg Principles on National Security, Freedom of Expression and Access to Information" adopted by a group of experts convened by Article 19 in 1995, and the "Principles of Oversight and Accountability for Security Services in a Constitutional Democracy" elaborated in 1997 by the Centre for National Security Studies (CNSS) and the Polish Helsinki Foundation for Human Rights.

[5] Paragraph 9 of the Joint Declaration stated that the law must clearly specify the criteria to be used for determining the cases in which such surveillance is legitimate for national security purposes and such measures shall be authorized only in the event of a clear risk to protected interests and when the damage that may result would be greater than society's general interest in maintaining the right to privacy and the free circulation of ideas and information. In any case, the collection of this information shall be monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society.

[6] A/RES/68/167. The resolution, which was co-sponsored by 57 Member States, was taken without a vote.

expressed deep concern at the negative impact that surveillance and interception of communications, including extraterritorial surveillance and interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights and urged States to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.

5. More specifically, on 26 March 2014, the Human Rights Committee, in its Concluding observations on the fourth report of the United States of America under the ICCPR[7], recommended that measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of the individuals whose communications are under direct surveillance. It also insisted on the need for reform of the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization or monitoring of surveillance measures, and considering the establishment of strong and independent oversight mandates with a view to preventing abuses.

6. On request of the General Assembly, the United Nations High Commissioner for Human Rights (UNHCHR), presented a report on 30 June 2014 on the right to privacy in the digital age[8]. The report dealt with the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and the interception of digital communications and the collection of personal data, including on a mass scale. Concerned with media revelations suggesting that the National Security Agency in the United States of America and the General Communications Headquarters in the United Kingdom had developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content and that these technologies had been deployed through a transnational network comprising strategic intelligence relationships between Governments, regulatory control of private companies and commercial contracts, the UNHCHR underscored that, other than the right to privacy, the rights to freedom of opinion and expression, and to seek, receive and impart information, to freedom of peaceful assembly and association and to family life may also be affected by mass surveillance, the interception of digital communications and the

---

[7] Human Rights Committee Concluding Observations on the 4th USA report, CCPR/C/USA/CO/4, 26 March 2014, para. 22(d).
[8] A/HRC/27/37.

collection of personal data. Targeted surveillance of digital communication may constitute a necessary and effective measure for intelligence and law enforcement entities when conducted in compliance with international and domestic law, but "it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate". Mandatory third-party data retention, whereby Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access, appears neither necessary nor proportionate. With the line between criminal justice and protection of national security blurring significantly, the sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating the right to privacy, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another. Thus, States should take steps to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy[9].

7. More recently, on 24 March 2015, the Human Rights Council decided to appoint, for a period of three years, a special rapporteur on the right to privacy[10].

8. Within the Council of Europe, the disclosure of the mass surveillance practices raised a renewed interest on the Convention for the protection of Individuals with regard to automatic processing of personal data, of 28 January 1981[11], and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows of 8 November 2001[12], as well as the Committee of Ministers Recommendation No. R (87) 15, on the use of personal data in the police sector, adopted on 17 September 1987, and Recommendation No. R (95) 4, on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, adopted on 7 February 1995, and the Parliamentary Assembly (PACE) Recommendation 1402(1999)1, on the control of internal security services in Council of Europe member states, adopted on 26 April 1999[13]. Additionally, both the Venice

[9] Paragraphs 24-27 and 50 of the report.
[10] A/HRC/28/L.27.
[11] ETS no. 108.
[12] ETS no. 181.
[13] The PACE expressed its clear preference for extensive a priori and ex post facto judicial control of surveillance activities with a high potential to infringe upon human rights, on the basis of "probable cause for belief that an individual is committing, has committed, or is about to commit an offence", or "probable cause for belief that particular communications or specific proof concerning that offence will be obtained through the proposed interception

Commission report on the democratic oversight of the security services, adopted in June 2007[14], and the European Commission against Racism (ECRI) General Policy Recommendation no. 11 on combating racism and racial discrimination in policing, adopted on 29 June 2007, gained new actuality[15].

9. Immediately after the publication of the Snowden files, the Committee of Ministers adopted the "Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies", of 11 June 2013, followed by the PACE Recommendation (2024)2013[16] and Resolution (1954)2013 on national security and the right to information, adopted both on 2 October 2013[17], and the Commissioner for Human Rights comment on "human rights at risk when secret surveillance spreads", of 24 October 2013, and issue paper "The rule of law on the internet and in the wider digital world", of 8 December 2014[18].

10. More recently, in March 2015, the Venice Commission adopted the "Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies", which distinguishes between targeted surveillance (covert collection of conversations, telecommunications and metadata) and "strategic surveillance" which "does not necessarily start with a suspicion against a particular person or persons". The Commission insists on a system

---

or house searches, or that (in the case of arrest) a crime can thus be prevented" and "normal investigative procedures have been attempted but have failed or appear unlikely to succeed or be too dangerous." The authorisation to undertake this kind of operative activity should be time-limited (to a maximum of three months). Once observation or wire-tapping has ended, the person concerned should be informed of the measure taken.

[14] CDL-AD(2007)016-e. The Venice Commission stated its preference for judicial authorization and review of surveillance operations directed to "individual cases", but noting at the same time that much surveillance work is not directed towards pre-trial legal procedures, such as data-mining, and this kind of surveillance work tends to escape judicial control (paras. 29, 202-204). Finally, it conceded that "there may not be much in the way of concrete suspicions to go on at the time when surveillance is requested but other means of obtaining information may be regarded as impracticable." (para. 207).

[15] CRI(2007)39. The ECRI called on the Governments to introduce a reasonable suspicion standard, whereby powers relating to control, surveillance or investigation activities can only be exercised on the basis of a suspicion that is founded on objective criteria.

[16] The Recommendation encouraged member States of the Council of Europe to take into account the Tshwane Principles.

[17] The Resolution affirmed that the neutrality of the Internet requires that public authorities, Internet service providers and others abstain from using invasive wiretapping technologies, such as deep packet inspection, or from otherwise interfering with the data traffic of Internet users.

[18] CommDH/IssuePaper(2014)1. The Commissioner defended that "suspicionless mass retention of communications data" is fundamentally contrary to the rule of law, incompatible with core data-protection principles and ineffective. Member states should not resort to it or impose compulsory retention of data by third parties.

of judicial authorization complemented by some form of follow-up control that conditions are being complied with. The power to "contact chain", i.e. identify people in contact with each other, should be framed narrowly: contact chaining of metadata should normally only be possible for people suspected of "actual involvement in particularly seriously offences", such as terrorism. Strengthened justification requirements and procedural safeguards should apply, such as the involvement of a privacy advocate, with regard to searches of content data. In the view of the Commission, notification that one has been subject to strategic surveillance is not an absolute requirement of Article 8 of the Convention. If a state has a general complaints procedure to an independent oversight body, this can compensate for non-notification[19].

11. On 21 April 2015, the PACE approved Resolution 2045(2015) on mass surveillance, urging the Council of Europe member and observer States to ensure that their national laws only allow for the collection and analysis of personal data, including metadata, with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity.

12. In May 2015, the Council of Europe Commissioner for Human Rights published an issue paper on "Democratic and effective oversight of national security services", advocating that independent *ex ante* authorisation should be extended to untargeted bulk collection of information, the collection of and access to communications data, including when held by the private sector, and, potentially, computer network exploitation. The process by which intrusive measures are authorised or re-authorised should itself be subject to scrutiny. States must ensure that individuals can also access a supervisory institution equipped to make legally binding orders.

13. Reacting to the worldwide debate on mass surveillance, the European Union (EU) did not speak with one voice. The first institutional position came from the European Commission, with its Communications to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established[20], and on "Restoring Trust in EU-US data flows"[21], both of 27 November 2013. Following the *Schrems* judgment by the Court of Justice, the Commission delivered a Communication to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United

---

[19] CDL-AD(2015)006, paragraphs 3, 16, 24, 51, and 103-105.

[20] COM(2013) 847 final. The Commission identified a number of shortcomings and set out 13 recommendations. On the basis of these recommendations, the Commission held talks with the U.S. authorities since January 2014 with the aim of putting in place a renewed and stronger arrangement for transatlantic data exchanges.

[21] COM(2013) 846 final.

States of America under Directive 95/46/EC, on 6 November 2015, insisting that a renewed and sound framework for transfers of personal data to the United States remains a key priority for the Commission, but at the same time identifying alternative, vg. contractual, tools authorising data flows by companies for lawful data transfers to third countries like the United States.

14. By its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs[22], the European Parliament condemned virulently the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information, in an "indiscriminate and non-suspicion-based manner", calling EU Member States to ensure that their intelligence services be subject to parliamentary and judicial oversight and public scrutiny and that they respect the principles of legality, necessity, proportionality, due process, user notification and transparency. In the framework of the relations between the EU and the US, the European Parliament specifically required that effective guarantees be given to Europeans to ensure that the use of surveillance and data processing for foreign intelligence purposes is proportional, limited by clearly specified conditions, and related to reasonable suspicion and probable cause of terrorist activity, stressing that this purpose must be subject to transparent judicial oversight. One year later, the European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014[23], called on the Commission to prepare guidelines for Member States on how to bring any instruments of personal data collection for the purpose of the prevention, detection, investigation and prosecution of criminal offences, including terrorism, in line with the judgments of the Court of Justice on data retention and on Safe Harbour, pointing in particular to paragraphs 58 and 59 of the data retention judgment and to paragraphs 93 and 94 of the Safe Harbour judgment, which, in the parliamentarians view, clearly demand a targeted approach for data collection rather than a 'full take'. It further warned against the obvious downward spiral for the fundamental right to privacy and personal data protection occurring when every bit of information on human behaviour is considered to be potentially useful in combating future criminal acts, necessarily resulting in a mass surveillance culture where every citizen is treated as a potential suspect and leading to the corrosion of societal coherence and trust.

---

[22] 20013/20188(INI). This Resolution was anticipated by the important "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Afairs" (A7-0139/2014), of 21 February 2014

[23] 2015/2635(RSP).

15. As a matter of fact, the Luxembourg Court played a major role in redefining the limits of covert data gathering for national security purposes in the EU and outside it. In *Maximillian Schrems v Data Protection Commissioner*[24], the Court of Justice of the European Union declared that the Commission's US Safe Harbour Decision is invalid, because it authorises, on a generalised basis, storage of all the personal data of all the persons whose data is transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use. The Court added that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life. Likewise, the Court observed that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law. Finally, the Court found that the Safe Harbour Decision denies the national data protection supervisory authorities their powers where a person calls into question whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals. The Court held that the Commission did not have competence to restrict the national supervisory authorities' powers in that way.

In the joint cases of *Digital Rights Ireland* and *Seitinger and Others*[25], the Luxembourg Court had already declared invalid the Data Retention Directive 2006/24/EC laying down the obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data (or metadata) for periods from six months to two years, in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. Both individually and in the aggregate, these surveillance capabilities allowed the state to build a precise picture of the most intimate aspects of an individual's life. The potential threat to privacy resulting from such compulsory, suspicionless, untargeted data retention obligation, generating in the minds of the persons concerned the feeling that their

[24] Case C-362/14, judgment of 6 October 2015.
[25] Cases C-293/12 and C-594/12, judgment of 8 April 2014.

private lives were subject to constant surveillance, breached Articles 7 and 8 of the EU Charter on Fundamental Rights[26].

16. Finally, the European Data Protection Authorities made known their views on the threats to privacy resulting from mass surveillance tools. The European Data Protection Supervisor delivered, on 20 February 2014, an Opinion on the Communications from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU"[27]. Subsequently, the Working Party Article 29 published its Opinion 4/2014 on surveillance of electronic communications for intelligence and national security purposes, of 10 April 2014[28]. On 26 November 2014, the European Data Protection Authorities Assembled in the Article 29 Working Party issued a Joint Statement[29].

Application of the international law standards to the facts of the case

The categories of offences or activities surveilled

17. Act no. XXXIV of 1994 on the Police (the Police Act) does not contain any definition of a "terrorist act" or "terrorist action", which could eventually raise a problem in terms of foreseeability of the legal framework of intelligence gathering for national security purposes under Section 7/E (3). It can be argued that the reference of Section 69 (5) to "terrorist acts (Section 261 CC)" fills the definitional gap and consequently that these concepts refer to the definitions of the Criminal Code, as paragraph 64 of the judgement pretends[30]. Hence, the safeguard mentioned in paragraph 231 of *Roman Zakharov* ("the nature of offences which may give rise to an

---

[26] The Luxembourg Court was clearly inspired by the standard established in the data retention directive case in Germany in 2010 (BVerfG 125, 260).
[27] 2014/C 116/04.
[28] 819/14/EN. While focusing on the access to metadata, the Working Party concluded that secret, massive and indiscriminate surveillance programs are incompatible with the EU fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. The Working Party, amongst others, called for effective, robust and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself. The recommendations of the Opinion were based on the legal analysis published in the Working Document on surveillance of electronic communications for intelligence and national security purposes, of 5 December 2014.
[29] 14/EN WP227.
[30] Paragraph 64 of the judgment.

interception order") is set out in the Hungarian law with the necessary degree of clarity and precision[31].

The degree of suspicion of involvement in the offences or activities surveilled

18. Act no. CXXXV of 1995 on National Security Services (the National Security Act) does not contain any requirement that the persons surveilled must be under a "reasonable suspicion" standard, which contradicts the standard for authorizing secret surveillance set out in paragraphs 260, 262 and 263 of *Roman Zakharov* and previously in paragraph 51 of *Iordachi and Others*[32]. The only standard established by the Hungarian law is that of the "persons concerned identified by name or as a range of persons" (Section 57 (2) (a) of the National Security Act), which

---

[31] See also my separate opinion in *Draksas*, cited above, page 26, point (2). Hence, I cannot share the Chamber's statement that "the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations" (§ 64), which not only downgrades the role of the principle of legality in a field of law where its rigorous reading is most needed, but also leaves the door wide open to the Ministry of Justice creative interpretation of the law and therefore to State abuse. An example of this worrying creative interpretation is given by the Government themselves in the present case, which refer to the two following tasks pursued by secret intelligence gathering subject to ministerial authorization in Hungary: "one the one hand, to detect and eliminate acts of terrorism and, on the other hand, to find and rescue Hungarian nationals got in trouble in a foreign country. The applicants may only be regarded to be affected by the contested provisions in so much that the Act does not exclude them from the circle of persons who in the context of the detection and identification of a person or a group of persons potentially linked to an act of terrorism may, among the persons or at a location or in a facility endangered by an act of terrorism, be affected by secret intelligence gathering…" (page 8 of the Government observations of 31 October 2014). This means that any person with a "potential link" to an act of terrorism or a place endangered by an act of terrorism, including the potential victims, may be submitted to a surveillance measure, as well as any person potentially linked to an incident with an Hungarian who "got in trouble in a foreign country"! In their security-purposed logic, the Government conclude that "the national security aspects to be weighed can be specified under the law in very broad terms, as in the actual assessment security policy aspects, that is non-legal aspects will have priority… In the field of authorizing national security-purposed secret intelligence gathering no positive law specifying an exact criteria system providing grounds for a judicial decision exists or can be created. (…) Therefore in the field of combatting terrorism authorization for national security-purposed secret intelligence gathering is granted on the basis of a politically influenced criteria-system which cannot be specified under positive law…" (page 12 of the Observations). Summing up the Government's perspective, State secret surveillance is the realm of politics and no law "exits or can be created" to limit this realm.

[32] *Iordachi and Others v. Moldova*, no. 25198/02, 10 February 2009. See also my separate opinion in *Draksas*, cited above, pages 26, point (3), and page 27, for similar defects of the Lithuanian law.

inevitably allows for unfettered ministerial discretion and for a "strategic, large-scale interception"[33]. In paragraph 71 of the present judgment, the Chamber chose the lower standard of an unqualified "individual suspicion", which diminishes significantly the degree of protection set out in *Roman Zakharov* and previously in *Iordachi and Others*[34]. Worse still, the almost evanescent suspicion criterion chosen by the Chamber is totally at odds with the growing concern of the United Nations, the Council of Europe and the European Union with massive, indiscriminate and secret "bulk surveillance" and the present state of international law, as established in the above mentioned documents, like the Parliamentary Assembly Resolution 2045(2015) and its Recommendation 1402(1999)1, the Venice Commission 2007 and 2015 reports, the European Commission against Racism General Policy Recommendation no. 11 and the European Parliament Resolutions of 12 March 2014 and of 29 October 2015.

19. Implicit in the Chamber's reasoning, as well as in the Constitutional Court's, is the assumption that national security protection is not limited to the investigation of past, ongoing or future offences and therefore the "reasonable suspicion" should be dispensed with. This assumption is wrong in the present case, in face of the letter of Section 7/E (3) of the Police Act, which specifically refers to preventing, tracking and repealing of attempts to carry out terrorist acts in Hungary (subsection (1) point a) sub-point ad)) and to rescuing Hungarian citizens who are in distress due to an imminent and life-threatening danger of act of war, armed conflict, hostage-taking or terrorist action outside the territory of Hungary (subsection (1) point (e)). As it is plain to see, these tasks refer either to criminal prevention of acts of terrorism in Hungary or rescue operations of situations of danger, war, armed conflict, hostage-taking or terrorist action already ongoing outside the territory of Hungary. In both cases of criminal prevention and rescue operations, nothing hinders the applicability of the criterion of "reasonable suspicion" of involvement of the targeted surveilled person in terrorist acts or the situation of danger when collecting secret intelligence useful for the performance of those tasks.

---

[33] The critique of the Chamber in paragraph 69 of the judgment is entirely right, but unfortunately the Chamber did not follow to the end this logic.

[34] In other words, the Chamber standard is even below the lowest degree of *bona fide* suspicion or "initial suspicion" (*Anfangsverdacht*) relevant in criminal law. The Chamber's mentioning of paragraphs 259 and 261 of *Zakharov* is misleading, since the Grand Chamber qualified the "individual suspicion" by restricting it to a "reasonable suspicion" test in paragraphs 260, 262 and 263, which the Chamber chose to ignore. Furthermore, the Chamber's reference to a "sufficient factual basis" adds nothing, because this evidentiary "basis" refers to the "supportive materials" and not to the degree of suspicion required to justify the application of any secret intelligence gathering measure. For further discussion on the three possible degrees of suspicion in the field of criminal law, see my separate opinion in *Lagutin and Others*, cited above, page 38, point 9.1).

20. The real reason why the Chamber's reasoning does not remain faithful to the Grand Chamber's criterion of "reasonable suspicion" is because it assumes that the fight against terrorism requires a "pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks"[35]. The vagueness of this language is impressive, encapsulating the net-widening, all-inclusive, minimalist suspicion threshold supposedly needed to fight efficiently terrorism. By so doing, the Chamber ignores that "The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other."[36] Furthermore, such optimistic language is indicative of an illusory conviction that global surveillance is the *deus ex machina* capable of combating the scourge of global terrorism. Even worse, such delusory language obliterates that a vitrified society brings with it the 1984 Orwelian nightmare. In practice, the Chamber is condoning, to use the words of the European Parliament, "the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence"[37].

The necessity test

21. Section 53 of the National Security Act provides for the necessity test. Paragraphs 67, 71, 72, 74, 75 and 88 of the judgment use a "strict necessity" test and refer it to two purposes: safeguarding of democratic institutions and obtaining of vital intelligence in an individual operation[38]. This creative rephrasing of the legal test raises several problems. Firstly, it is a stricter criterion than the one of paragraphs 233 and 236 of

---

[35] Paragraph 78 of the judgment.

[36] *Liberty and Others v. the United Kingdom*, no. 58243/00, § 63, 1 July 2008, and *Weber and Saravia v. Germany (dec.)*, no. 54934/00, § 114, 29 June 2006, both concerned with generalised "strategic monitoring".

[37] Paragraph 12 of the European Parliament Resolution of 12March 2014, cited above.

[38] In fact, the Chamber uses a double language. Paragraph 58 refers to the "necessity" test and the "necessity" requirements, but subsequently the language becomes more demanding, adding the adjective "strict" to the word necessity.

Roman Zakharov[39]. Secondly, it does not match with the looser criterion for the degree of suspicion of involvement in the offences or activities surveilled. It is logically inconsistent that the same judgment imposes a "strict necessity" test for the determination of the surveillance measure, but at the same time admits a very loose criterion for the degree of suspicion of involvement in the offences or activities surveilled, as demonstrated above. It is logically incoherent to criticise the overly broad text of the Hungarian law when it refers to the "persons concerned identified as a range of persons" and accept the linguistically vague and legally imprecise "individual suspicion" test to ground the applicability of a surveillance measure. Thirdly, the Chamber did not clarify in what consists the "strict necessity test", having merely linked the test to the purposes pursued. Nowhere in the judgment is clarified that the necessity test warrants that any surveillance operation be ordered only if the establishment of the facts by other less intrusive methods has proven unsuccessful or, exceptionally, if other less intrusive methods are deemed unlikely to succeed[40].

The list of special surveillance techniques and their maximum duration

22. Section 56 of the National Security Act provides an exhaustive list of special investigation techniques, which include search and surveillance of dwellings, mail and electronic communications' interception and computer and network data interception. But Section 58 does not provide a maximum time limit for the surveillance measures, as paragraph 231 of *Roman Zakharov* requested[41]. It only foresees the maximum period of 90 days for each request, with the possibility of unlimited renewals being open to the Minister of Justice. Furthermore, the Minister of Justice has no access to the results of the ongoing surveillance when called on to decide on its prolongation, which evidently facilitates the mere rubber-stamping of the prolongation request.

The authorization and review procedure

23. The National Security Act does not provide for an independent authority to authorize the beginning of the surveillance operation (first stage or *ex ante* review stage), since Section 58 only refers to the Minister of Justice as the sole authority to decide over the motion for a secret

---

[39] *Roman Zakharov*, cited above, § 233 ("the bounds of necessity, within the meaning of article 8 § 2") and § 236 ("the necessity test", "to address jointly the "in accordance with the law" and "necessity" requirements").

[40] See my separate opinion in *Draksas*, cited above, page 26, point (4), and my separate opinion in *Lagutin and Others*, cited above, page 36, point (6).

[41] See my separate opinion in *Draksas*, cited above, page 26, point (5).

surveillance measure, without further appeal against his or her decision being admissible[42]. The legal framework does not include the examination of the case file and the assessment of the factual and legal grounds for auhorisation of the secret surveillance measure by an independent authority, preferably a judge, as paragraph 233 of *Roman Zakharov* stated, following *Klass and Others*[43]. In view of the enlarged consensus in international law mentioned above and the gravity of the present-day dangers to citizens' privacy, the rule of law and democracy, the time has come not to dispense with the fundamental guarantee of judicial autorisation and review in the field of covert surveillance gathering[44]. Obviously, the judicial guarantee is not incongruous with an additional external guarantee of political, vg parliamentarian, nature.

24. In the case at hand, the Parliament's National Security Committee and the Commissioner for Fundamental Rights external control does not guarantee an independent evaluation of the ministerial exercise of decisional powers, in view of the absence of review powers of the external supervisory entities themselves in concrete cases[45]. In addition, in the course of his or her inquiry affecting the national security services, the Commissioner for Fundamental Rights is deprived of almost all relevant documentation, since he or she may not inspect registers for the identification of individuals cooperating with the national security services, documents containing the technical data of devices and methods used by the national security services

---

[42] On the three stages of the oversight procedure, when the surveillance is first ordered, while it is being carried out and after it has been terminated, see paragraph 233 of *Roman Zakharov*, cited above, as well as paragraph 72 of the Decision no. 32/2013 (XI.22) AB of the Constitutional Court, cited in paragraph 20 of the judgment above.

[43] *Klass and Others v. Germany*, 6 September 1978, §§ 55 and 56, Series A, no. 28.

[44] See also my separate opinion in *Draksas*, cited above, page 26, point (6). I cannot thus follow the Hungarian Constitutional Court, when it argues that "Identifying and combating endeveaours aimed at committing acts having relevance from the aspects of securing the sovereignty of the State and of protecting the lawful order of the State may fall outside the sphere of particular criminal offences. (…) The prevention and elimination of risks to national security require political decisions, therefore decisions of this type fall in the competence of the executive power" (paragraph 105 of the Decision no. 32/2013 (XI.22) AB of the Constitutional Court, cited in paragraph 20 of the judgment above). Neither can I accept the argument of the Government that judges are not welcomed, "because either due to lack of expertise or the absence of external – political – accountability on the part of the courts or – in case of specilisation – due to the courts' becoming part of the system and their resulting readiness to give preference to national security interests, courts tend to accept the risk-assessments of the national security services, hence judicial control constitutes only formal supervision." (Government observations of 31 October 2014, page 11).

[45] Although the Committee may request information on particular cases under Section 14 (4) a) of the National Security Act, and the Minister or the chief director shall, within the established deadline, reply, the Committee lacks any decision-making power with regard to the particular cases.

for intelligence information gathering, or documents making it possible to identify the persons using them, documents relating to encryption activities and encoding, security documents relating to the installations and staff of the national security services, documents related to security documents and technological control, documents access to which would make possible the identification of the source of the information, or documents access to which would infringe the obligations undertaken by the national security services towards foreign partner services[46].

25. The shortcomings of the external political control are correctly criticized by the Chamber, but the reasoning of the judgment omits a holistic assessment of the subsequent surveillance review procedure, which is essential to assess if the overall fairness of the system put in place by the Hungarian legislator compensates the shortcomings of the first stage of the secret intelligence gathering procedure[47].

26. The National Security Act does not establish an independent (ie, judicial) authority to monitor and review pending the surveillance operation (second stage or implementation stage) such matters as whether the secret services are in fact complying with the decision authorising the use of secret operational measures, whether they faithfully reproduce in the records the original data obtained during the operation and whether the surveillance remains necessary for the performance of the tasks specified in the law, as paragraph 251 of *Roman Zakharov* underscores[48].

27. In addition, when the surveillance operation is over (third stage or *ex post* review stage), there is no provision for acquainting an independent (ie, judicial) authority with the results of the surveillance and the law does not

---

[46] Article 23 (2) of the Act CXI of 2011 on the Commissioner for Fundamental Rights. This contradicts the principle that oversight institutions should have the power to initiate their own investigations into areas of the intelligence service's work that fall under their mandates, and are granted access to all information necessary to do so (see UN 2010 Compilation of good practices, cited above, para. 14, and the UNHCHR 2014 report, cited above, para. 41). In fact, the practice has been that the Ombudsman's office never dealt with a case on the surveillance of citizen (paragraph 18 of the judgment and annex 2 to the applicants' observations).

[47] A similar holistic assessment of the Russian law was made by the Grand Chamber in *Roman Zakharov*, cited above, § 178. The Hungarian Constitutional Court examined both the autorisation stage and the handling of the collected data following the termination of the interference and found the protection of the right to privacy satisfactory in the light of the guarantees subsequent to the autorisation stage, such as the parliamentary external oversight. The Government themselves referred to these guarantees in paragraphs 16 to 18 of their observations. Although the Chamber considered, in paragraph 58 of the judgment, that "the Court is required to examine this legislation itself and the safeguards built into the system allowing for secret surveillance", it did not deliver what it promised.

[48] In paragraph 274 of *Roman Zakharov*, cited above, the Court noted that the domestic courts had no competence to supervise the implementation stage of the secret surveillance measure, finding in paragraph 285 that the supervision of this second stage by the public prosecutor was insufficient.

compel this authority to review whether the requirements of the law have been complied with. There are no regulations specifying with an appropriate degree of precision the manner for screening the original data obtained through surveillance, the procedures for preserving its integrity and confidentiality and the procedure for its destruction[49]. Similarly, there exists no independent review of whether the original data are in fact destroyed within a time-limit if the surveillance has proved fruitless[50].

The urgent procedure

28. An urgent procedure may be decided by a non-independent authority, like the director of the national secret services, only where the normal procedure would entail a delay that would render useless the operation. Section 59 of the National Security Act refers to "if the external authorisation procedure entails such delay as obviously countering, in the given circumstances, the interests of the successful functioning of the National Security Service". But it does not limit the use of the urgency procedure to cases involving an immediate serious danger to national security. Furthermore, it does not provide that the director's decision be within a short period of time confirmed by an independent (ie, judicial) authority, with full reviewing power, as established in paragraph 266 of *Roman Zakharov* and previously in paragraph 16 of *Association for European Integration and Human Rights and Ekimzhiev*[51], since the director's decision may only be confirmed or not by the Minister of Justice within 72 hours.

The communication of the obtained data to third parties

29. The National Security Act does not set out the conditions to be fulfilled and the precautions to be taken when the National Security

---

[49] The interpretation proposed by the Constitutional Court in paragraph 138 of the Decision no. 32/2013 (XI.22) AB of the Constitutional Court, cited in paragraph 20 of the judgment above, deriving from sections 43 and 50 (2) (e), when read in conjunction, a legal obligation to delete ex officio unnecessary data not only seems forced, but does not really solve the issue, since no specifics are provided about the competence, timing and procedure for deletion of data collected for the purposes of Section 7/E (3) of the Police Act.

[50] See my separate opinion in *Draksas*, cited above, page 28, for similar defects in the Lithuanian law. Paragraph 255 of *Roman Zakharov*, cited above, censured the automatic storage for six months of clearly irrelevant data. But the Grand Chamber did not take in account the interest of the surveilled person to invoke the allegedly "irrelevant" data in his or her defence, as quite rightly argued in *Dumitru Popescu v. Romania (no. 2)*, no 71525/01, § 78, 26 April 2007.

[51] *European Integration and Human Rights and Ekimzhiev v Bulgaria*, no. 62540/00, § 16, 28 June 2007.

Services communicate the obtained data to third parties, as paragraph 231 of *Roman Zakharov* specifically requests[52]. The vague reference of Section 45 to the transferal of personal data to "foreign data processing authorities within the framework of laws on protection of personal data" is manifestly insufficient.

The duty to notify the person under surveillance

30. The National Security Act does not establish the duty to notify the person under surveillance of the measure taken when it is over, provided that the interests of national security are not endangered by such disclosure, as paragraph 234 of *Roman Zakharov* determines, following here again *Klass and Others*[53]. No special guarantees with regard to the secrecy of lawyer-client, doctor-patient, priest-penitent and journalist-source privileged communications are included in the Hungarian legal regime either[54].

The lack of effective remedies

31. Section 58 of the National Security Act prohibits appeals against the Minister of Justice decision on any motion for a covert surveillance measure under Section 7/E (3) of the Police Act. The absence of any *ex post facto* notification aggravates the situation of helplessness of the surveilled persons. Hence, the complaint procedure outlined in Sections 11 (5) and 14 (4) (c) to (f) of the National Security Act provides a merely virtual defence possibility to the surveilled persons[55]. Consequently, persons under surveillance in Hungary, like in Russia, have no real possibility of lodging

---

[52] See also my separate opinion in *Draksas*, cited above, page 26, point (8).

[53] *Klass and Others*, cited above, §§ 55 and 56. See also my separate opinion in *Draksas*, cited above, page 26, point (9), and page 29 for similar defects of the Lithuanian law.

[54] See also my separate opinion in *Draksas*, cited above, page 26, point (10). The Parliamentary Assembly Resolution 1954 (2013), cited above, reiterated that measures such as interception orders or actions concerning communication or correspondence of journalists or their employers or surveillance orders or actions concerning journalists, their contacts or their employers should not be applied if their purpose is to circumvent the right of journalists not to disclose information identifying a source. The Venice Commission underscored very recently the "particularly problematic" nature of interception of privileged communications by means of covert intelligence of lawyers, priests or journalists and gave the example of covert surveillance of journalists in order to identify their sources (Venice Commission Update of the 2007 report, cited above, paras. 18 and 106-108).

[55] This is confirmed by the inexistence of complaints to the National Security Commission (annex 1 of the applicants' observations, confirmed by the Government observations of 14 January 2015).

complaints, requests or appeals against concrete surveillance orders to which they have been subjected[56].

32. In the remote case that the concerned person does take knowledge of the surveillance measure issued in his or her regard, for example, where he or she received leaked information confirming the measure, the domestic complaint procedure does not ensure an independent and effective assessment of the submitted grievances. In addition to what has already been said about the lack of decision-making powers of the Parliament's National Security Committee, it should be added that inquiries about complaints related to the activities of the national security services are initially conducted by the Minister of Home Affairs, who shall inform the complainants about the findings of the inquiry and the measures taken within 30 days procedure. The minister is evidently not an independent authority. If not satisfied, the complainant may appeal to the Committee, which may conduct inquiries if "the weight of the complaint, according to one third of the votes of the committee members, justifies the inquiry". The political nature of the Committee's decision is enhanced by the discretionary assessment of the "weight of the complaint" and the majority vote taken in order to open the inquiry. The Committee may conduct a fact-finding inquiry, in the course of which it may have access to the relevant documents kept in the registry of the national security services, and may hear the staff members of the national security services. If it concludes that the operation of the national security services is unlawful, or is contrary to their designated purpose in any manner, the Committee may only call upon the Minister to take the necessary measures. Hence, the remedial body is neither obligated to conduct an investigation nor to furnish effective redress, let alone to order the discontinuance of any ongoing abusive surveillance as well as the destruction of unlawful personal data. Ultimately, it is up to the Minister to decide what action, if any, he or she wants to take in reply to the complainant's grievances.

33. Furthermore, although Section 50 (2) (b) of the National Security Act mentions the possibility of deletion of personal data "ordered by a court in data protection proceedings", and section 48 allows for the "concerned persons to file a request for the deletion of their personal data"[57], it is not clear how the concerned surveilled person may request that his or her personal data be deleted if he or she does not even have a fair possibility of

---

[56] In Russia, the general remedies were only available to persons in the possession of information about the surveillance measure, and therefore their effectiveness was undermined by the absence of a requirement to notify the subject of the measure at any point (*Roman Zakharov*, cite above, § 298, and previously, *Association for European integration and Human rights and Ekimdzhiev*, cited above, § 100).

[57] See the Constitutional Court's interpretation of this provision in paragraph 138 of its Decision no. 32/2013 (XI.22) AB, cited in paragraph 20 of the judgment.

obtaining information about the collection of that personal data by the National Security Services.

34. In sum, by depriving the subject of the secret surveillance measure of any notification of its existence and therefore of the effective possibility of challenging it retrospectively, Hungarian law eschews the most important safeguard against improper use of secret surveillance measures[58]. Were Samuel Warren and Louis Brandeis confronted with law, they would undoubtedly repeat the words they used to call for their right to privacy: "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity so that solitude and privacy have become more essential to the individual"[59].

Conclusion

35. As a foundational matter, I recall that "a system of secret surveillance designed to protect national security entails a risk of undermining or even destroying democracy on the ground of defending it"[60]. Having this in mind, the Chamber quite rightly did not tone down the critique of the Hungarian legal framework on covert and massive surveillance in order to make it more palatable to the respondent Government. But if the tone is right, the substance of the judgment risks not to allay entirely the serious dangers for the citizens' privacy, the rule of law and democracy resulting from such legal framework[61]. Worse still, the choices made by the Chamber introduce a strong dissonant note in the Court's case-law. Paragraph 71 of the judgment departs clearly from paragraphs 260, 262 and 263 of *Roman Zakharov* and paragraph 51 of *Iordachi and Others v. Moldova*, since the Chamber uses a vague, anodyne, unqualified "individual suspicion" to apply the secret intelligence gathering

---

[58] I can therefore not agree with the Constitutional Court's statement that "Since secret intelligence gathering does, per definition, exclude the possibility of an effective remedy…" (see paragraph 72 of the Decision no. 32/2013 (XI.22) AB of the Constitutional Court, cited in paragraph 20 of the judgment above).

[59] Samuel Warren and Louis Brandeis, "The right to privacy", in Harvard Law Review, volume IV, no. 5, 15 December 1890, p. 196.

[60] *Rotaru v. Romania (GC)*, no. 28341/95,§ 59, 5 May 2000, paraphrasing *Klass and Others*, cited above, § 49: "The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."

[61] This is particularly worrying if one considers that over the past few years, several privacy and digital rights organizations have pointed to evidence that the Hungarian authorities have purchased potentially invasive surveillance technologies (Freedom House, Freedom on the internet, report on Hungary, 2015, page 15).

measure, while the Grand Chamber uses the precise, demanding, qualified criterion of "reasonable suspicion". Judicial authorization and review is watered down if coupled with the Chamber's ubiquitous criterion, because any kind of "suspicion" will suffice to launch the heavy artillery of State mass surveillance on citizens, with the evident risk of the judge becoming a mere rubber-stamper of the governmental social control strategy. A ubiquitous "individual suspicion" equates to overall suspicion, i.e., to the irrelevance of the suspicion test at all. In practice, the Chamber condones *volenti nolenti* widespread, non-(reasonable) suspicion-based, "strategic surveillance" for the purposes of national security, in spite of the straightforward rebuke that this method of covert intelligence gathering for "national, military, economic or ecological security" purposes received from the Grand Chamber in *Roman Zakharov*. Only the intervention of the Grand Chamber will put again things right.