Emese Pásztor*

Secret Intelligence Gathering – a Low Threshold Still Too High to Reach**

The Gap Between the Level of Privacy Protection in Europe and in Hungary After the Case of *Szabó and Vissy v Hungary*[1]

Security society, safety state,[2] garrison state[3] and even illiberal state[4] are terms referring to phenomena that were unavoidable in the last few years all over the globe, especially after 9/11. Even if these terms capture different aspects of a possible outcome to which the world is getting closer, the tendency to trivialise and under-estimate the importance of liberty seems to be the link connecting them. As Glenn Greenwald summarised Foucault's hypothesis in his TED talk[5] 'surveillance creates a prison in the mind that is a much more subtle though much more effective means of fostering compliance with social norms or with social orthodoxy, much more effective than brute force could ever be.'

But why would Hungary, a country never really concerned by terrorism, be important for understanding this tendency? From this very angle, Hungary seems to be a country particularly worth dealing with as – the former happiest barrack in the socialist camp,[6] the wunderkind of the democratic transition of Soviet satellites,[7] and later, the pioneer of unorthodox economic policies and illiberalism – was always gifted at keeping up with the zeitgeist quicker than the others. The pattern of democratic backsliding was already successfully implemented by Poland and one can never know who will be the next.

* Emese Pásztor (LL.M., PhD Candidate) is a junior assistant professor at the Constitutional Law Department of the Faculty of Law of ELTE University.

** Firstly, I would like to express my gratitude to my advisor Dr. Nóra Chronowski, associate professor at the Department of Constitutional Law of ELTE University for her support and valuable comments on the manuscript.

1 *Szabó and Vissy v Hungary,* no. 37138/14, 12 January 2016.

2 Charles D. Raab, 'Governing the Safety State' (Inaugural Speech, University of Edinburgh, 7 June 2005).

3 Harold D. Lasswell, 'The Garrison State' (1941) 46 (4) American Journal of Sociology 455–468.

4 Fareed Zakaria, 'The Rise of Illiberal Democracy' (1997) 76 (6) Foreign Affairs 22–43 <http://www.seep.ceu.hu/alpsa/articles/zakaria.pdf> accessed 2 May 2018.

5 <https://www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript?language=hu> accessed 2 May 2018.

6 <https://en.wikipedia.org/wiki/Goulash_Communism> accessed 2 May 2018.

7 Miszlivetz Ferenc, 'The Tunnel at the end of the light: The crisis of transition in Hungary' [2009] <http://www.kx.hu/ kepek/ises/anyagok/Tunnel_at_the_End_of_the_Light.pdf> accessed 2 May 2018.

Whether Hungary slides self- or even unconsciously on this slippery slope of anti-democratisation, from now on – in particular cases – there is definitely a difference between the level of protection provided by the European standard and the domestic institutions responsible for fundamental rights protection in Hungary, and not in favour of the latter. Presuming that Europe is not founded on the idea of division but of unity, to avoid such gaps widening further in any sense is crucial for maintaining this entity we now know as Europe.[8]

Driven by this idea, the following short case study compares the different standards of the Constitutional Court[9] of Hungary and the European Court of Human Rights[10] concerning secret intelligence gathering – a core issue of personal liberty and security, providing an excellent opportunity to mind (and measure) this gap.

I Privacy vs Security – the End of a Paradigm?

Balancing privacy and security, or generally speaking, the 'balancing paradigm'[11] is a widespread approach in the field of privacy protection, especially in the context of the emerging intensity of the threat of terrorism. The trade-off – an expression widely used in professional literature but also in infotainment media – presents privacy and security as competing values, which might be only realised at the expense of each other, as a kind of virtual zero-sum game.[12] In other words, the concept refers to the necessity of giving up our privacy in the hope of being protected by the state from the danger around us, threatening our security. In a wider sense, the trade-off not only balances privacy and security, but rather these two values as the symbols of the best interest of the individual and society, presenting security as the incarnation of community well-being, and privacy as the obstacle of state actions which aim to support the community. Everyday political discourse tempted by populism refers to this relation – the opposition of privacy and security, the individual and the community – so naturally, as if it would be an unquestionable triviality.

The critics of trade-off are a mixed bunch, but the reasons behind rejecting the idea are mainly fed by two different types of arguments. The main difference between them might be captured in that they are challenging the trade-off within the logical structure of the model, without questioning the opposition of privacy and security, or they contest the opposition itself.

---

8 A reference to Brexit, initiated by the United Kingdom European Union membership referendum on 23 June, 2016 shall suffice.

9 Hereinafter referred to as Constitutional Court or CC.

10 Hereinafter referred to as ECtHR or the Court.

11 Charles D. Raab, 'From balancing to steering: new directions for data protection' in C. J. Bennett, R. Grant, (eds), *Visions of Privacy: Policy Choices for the Digital Age* (University of Toronto Press 1999, 68–93).

12 Bernadette Somody, Máté Szabó, Iván Székely, 'Moving away from the security-privacy trade-off: The use of the test of proportionality in decision support' in M. Friedewald, P. Burgess, J. Cas and R. Bellanova, W. Peissl (eds), *Surveillance, Privacy and Security: Citizens' Perspectives* (PRIO New Security Studies 2017, Routledge) 155.

The first approach – criticizing the trade-off *within the trade-off* – usually covers attempts to show how the balancing paradigm relativises the importance of privacy compared to security. Such attempts make us feel that taking a stand for the sake of privacy reflects egoism and selfishness opposed to the noble objective of the public good. Moore[13] challenges three rival arguments undermining the importance of privacy, all of which support security when balancing comes about. The first argument, 'just trust us,' tries to convince us about letting those exercising public power decide on how to strike the balance. The second, 'nothing to hide,' as referred to by Moore, claims that only those who are engaged in immoral and illegal activities should worry about being monitored; and finally 'security trumps' holds that security interests are weightier than privacy claims simply by their character. By presenting historical examples and experiences of the abuses related to, for example, the USA Patriot Act, Moore concludes that we have no reason to trust the decision makers, claiming that states would definitely not crave the blind trust of citizens in their surveillance politics if the decision makers really would have 'nothing to hide'.[14] As Moore is not a constitutional lawyer, it would be unfair to criticise him for the lack of arguments rooted deeply in constitutional law; however, he definitely would not argue if we say that trust in the state is completely alien from the essential nature of protecting fundamental rights. Fundamental rights – ultimately and using all means – are rights which have to be protected *from* the state, even if the protection is provided *by* the state itself. Later on, Moore makes a clear distinction between sensitive personal information and information which points towards criminal activity, and claims that sexual or medical history, for example, are simply out of the domain in which others might have right to access information.[15] As an illustration of how the two different arguments are blended into each other, Moore's objective is to 'strike an appropriate balance'[16] between privacy and security, which he desires to provide by introducing new safeguards, boosting the accountability of the surveillance power. In his struggle to reach the equilibrium, he argues that legal guarantees may promote privacy and security simultaneously, without realising that this means, of necessity, that privacy and security are certainly not positioned on the opposite sides of the seesaw.

Referring back to the presentation cited in the introduction of this paper, Greenwald points out that even people who say that they have nothing to hide put passwords on their email accounts and locks on their bathroom doors, proving with their actions that, in reality, they instinctively understand the primal importance of privacy. Greenwald stresses that when we are being monitored our behaviour changes dramatically. In this sense, it seems that surveillance is not only capable of revealing past actions we would like to hide, but also deters

[13] Adam D. Moore, 'Privacy, security, and government surveillance: Wikileaks and the new accountability' (2011) 25 (2) Public Affairs Quarterly 141–156.
[14] Moore (n 13) 142–145.
[15] Moore (n 13) 146.
[16] Moore (n 13) 148.

us from future choices, limiting our freedom of making decisions on our own (even non-criminal) actions. The same approach comes up in Westin's *Privacy and Freedom,*[17] when the author identifies the four different states of privacy, and argues that, beyond solitude, we can behave honestly only in the state of intimacy. This honesty doesn't refer to the readiness to commit terrorist attacks and engage in activities against the state, but the ability to be who we are, without the slightest urge to pretend anything.

Adding more volume to the first group of critics, Bárd[18] draws the attention to the fact that giving up fundamental rights (in our case, privacy), is always a slippery slope, which makes it almost impossible later to regain rights we have abandoned before. According to her, this slippery nature is reflected in the tendency for measures interfering into privacy to be increasingly intrusive, constantly widening the scope, time-frame and intensity of application. In Bárd's interpretation, actual rights are given up for the sake of perceived, future dangers, which subjects law-making to feelings and 'emotional demands'.[19]

Both groups of critics are convinced that the trade-off is false or at least grievously misleading, but the ones who doubt that privacy and security should be balanced against each other attack the bases of the model and definitely go farther than pointing out the disproportionalities within the paradigm itself. Among those who question the model in its entirety, it is widely recognized that the trade-off oversimplifies the relation between privacy and security. Somody, Szabó, Székely[20] and earlier, Regan[21] pointed out that there is a dynamic complexity between privacy and security, and a simple opposition cannot describe the multiple connections between the interests of these values. Borrowing a classic example, if the safety of our homes might be achieved by installing locks on the doors, enhancing security and privacy at the same time, who would opt for more CCTV cameras?[22] As Somody, Szabó and Székely emphasise, this tendency to trust in the false plainness of relations leads to the risk of eroding not just privacy, but even the values the trade-off is intended to protect, including democracy as well.

Even though that putting the trade-off into context would be hard to bypass in any professional discussion, the idea is surprisingly not reflected in the thinking of the general public. People do not consider privacy and security as competing values. Analysing the acceptance of surveillance-oriented security technologies, researchers found that, in the minds of citizens, privacy and security are not thought to be exchangeable goods that could be traded.[23]

---

17 Alan Westin, *Privacy and Freedom (*Atheneum 1967, New York).

18 Petra Bárd, 'Foreword' in Petra Bárd (ed), *The Rule of Law and Terrorism* (HVG-ORAC 2015, Budapest) 7–21.

19 Bárd (n 18) 7–8.

20 Somody, Szabó, Székely (n 12) 155.

21 Priscilla M. Regan, *Legislating Privacy. Technology, Social Values, and Public Policy* (University of North Carolina Press 2017, Chapel Hill – London).

22 Somody, Szabó, Székely (n 12) 156.

23 Vincenzo Pavone, Sarah Degli-Esposti, 'Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security' (2012) 21 Public Understanding of Science 556. And see also: Bernadette Somody, Máté Szabó, and Iván Székely 'Biztonság és magánélet – Az alkumodell megkérdőjelezése és meghaladása' (2017) 103 (3) Replika 31.

Probably it is Raab[24] who turns the trade-off upside down in the most ingenious way, when he argues that privacy and security are not just far from being opposing values, but they are essentially the same. According to Raab, privacy is a security value, and by necessity, a community value as, if we consider the public interest in a broader sense, without privacy, the public spheres and policies of democratic societies could not even function. Without individual participation, no public issues may exist.[25] On the other hand, Raab cites Neocleous[26] to illustrate that, from the end of the eighteenth century, freedom and safety were somewhat synonymous, where safety traditionally referred to the freedom of the individual to follow their own interests.

Raab has got the point, but his approach is still slightly instrumental, as he argues that privacy is important because of its usefulness in the process of democratic decision making. Privacy has an immanent value, which – according to some voices – must be treated as the cornerstone of the diverse structure of fundamental rights. Wachter[27] goes so far as to argue that privacy must be considered 'as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights', which warns us to remain alert in case there is any interference. Among other magic spells, balancing can easily serve as an ideology for legitimising unreasonable restrictions of privacy.[28]

As we saw above, fresh winds blow around the relationship between privacy and security within the academic literature. This short summary is intended to give a context for the standards to be compared below.

Studying the case of *Szabó and Vissy v Hungary*, one can get the impression that the motivations of the effective legal regulation of secret intelligence gathering in Hungary are rooted in the trade-off. To unveil my original hypothesis, my primal suspicion was that the relevant domestic legislation and the approach of the Hungarian Constitutional Court deserved to be criticised from this viewpoint. However, if we have a closer look at the European standard shaped mainly by the Strasbourg Court, we see that the Court basically stands on the same ground. Even if the demise of the trade-off is increasingly obvious in professional discussions, the ECtHR still balances privacy and security against each other, as reflections of individual and community interests. Judge Pinto de Albuquerque seemed to detect this obsolescence, when in his concurring opinion to *Szabó and Vissy*[29] he stressed

---

[24] Charles D. Raab, 'A magánszféra mint biztonsági érték' (2017) 103 (3) Replika 81–95. Translated to Hungarian by Viktor Berger from 'Privacy as a Security Value' in Jon Bing, Dag Wiese Schartum et al. (eds), *En Hyllest / A Tribute* (Gyldendal 2014, Oslo) 39–58.

[25] Raab (n 24) 86–87.

[26] Mark Neocleous, 'Security, Liberty and the Myth of Balance. Towards a Critique of Security Politics' (2007) 6 (2) Contemporary Political Theory 141–142.

[27] Sandra Wachter, 'Privacy: Primus Inter Pares – Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights' (2017) <https://ssrn.com/abstract=2903514> accessed 2 May 2018.

[28] Somody, Szabó, Székely (n 12) 156.

[29] *Szabó and Vissy v Hungary,* Concurring opinion of Judge Pinto De Albuquerque, Section 20.

that presuming 'global surveillance is the *deus ex machina* capable of combating the scourge of global terrorism' is nothing more than an illusory conviction.

We definitely will have to wait until the views of Albuquerque will become the mainstream of the European standard. However, even if the theoretical context of the Court is not the most up-to-date, it is still better to ensure respect for privacy through balancing, than knowingly reproducing the fear of terrorism and bypassing debates on the basis of a single, but unfounded reference to the trade-off.

II *Szabó and Vissy* – the Facts Behind

To protect democratic institutions from the threat of terrorism, states may use extraordinary measures for surveillance. Surveillance always poses a threat for privacy rights, but the degree of this threat depends on the nature of the exact measure taken. When we talk about surveillance for the sake of combatting terrorism, the character and volume of surveillance cannot be compared to when surveillance is used to foster the investigation of certain crimes. The attempt at 'combating terrorism' means far more than investigating specific terrorist activities. While in criminal investigation, data acquisition is always closely linked to the particular case, national security-driven secret intelligence gathering aims at storing data, acquired due its very nature and with a purpose considerably more difficult to grasp. This problem is aggravated by the fact that the technical possibilities barely limit the use of surveillance measures.

The effective Hungarian legal background, in the frameworks of secret intelligence gathering driven by national security, authorises the Counter Terrorism Centre,[30] the SWAT state agency of Hungary specialised in counter-terrorism, for almost every action we can imagine when we think about surveillance. To exercise these powers, no judicial authorisation is needed – surveillance might be conducted based on ministerial approval, which means that the state interference in question is not just carried out, but even granted by the executive power.

Both the Constitutional Court and the ECtHR decided upon the issue, examining similar implications of the same case based on the application of Szabó Máté and Vissy Beatrix, former researchers of a Hungarian policy institute.[31] The judgment of the ECtHR created a new situation, by pointing out the weaknesses of the effective domestic regulation, and establishing that Article 8 of the Convention has been violated. This case provides an excellent

[30] Terrorelhárítási Központ (TEK).

[31] The Eötvös Károly Policy Institute (EKINT) is a think tank that was created in 2003 in order to establish a novel, unconventional institutional framework for shaping democratic public affairs in Hungary. The Institute wishes to contribute to raising professional and general public awareness and to shaping the political agenda in issues with an impact on the quality of relations between citizens and public power. The author is also engaged in a working relationship with the Institute as a researcher.

opportunity to evaluate the Hungarian standard assessed by the relevant decision of the Constitutional Court, and to summarise the expectations drawn up by the case-law of the ECtHR.

The relevant legal background specifies two types of secret intelligence-gathering. The first one is linked to the investigation of particular crimes, while the second – secret intelligence gathering driven by national security – isn't. The distinction was made based on historical factors[32] bringing about the adoption of a system of divided authorisation, according to the following. When the aim is to detect criminal offences, secret intelligence gathering is authorised in the same way as it is regulated by Act XXXIV of 1994 on Police and Act XIX of 1998 on Criminal Proceedings. In this case, a judge, designated for this particular task, decides upon authorisation. Concerning the second type, where national security-related secret intelligence gathering belongs, surveillance shall be authorised by the Minister of Justice, and the whole process is based upon the provisions of Act CXXV of 1995 on National Security. The possible scope of the measure in question is quite opaque; the only significant guarantee applied by the act is that secret intelligence gathering may only be carried out if the data required to perform the statutory tasks cannot be obtained in any other manner. External control is provided in theory, as the Parliament's National Security Committee may exercise control over the authorisation process itself, and the Commissioner for Fundamental Rights[33] can also examine violations related to the anti-terrorist organ as well. However, as the applicants pointed out, neither the Commissioner nor the National Security Committee had ever brought up the underlying question (at least according to the data available to the general public).

By way of the latter – national security-purposed secret intelligence gathering – the Counter Terrorism Centre is entitled to conduct secret house searches, record all the data collected, open letters and parcels, and to check and record the content of electronic communication as well. As the use of these measures is secret, all this happens without the consent of the subject concerned.

[32] In January 1990, the 'Budapest Watergate' scandal broke out; this revealed that even after the democratic transition, the III/III Division of the internal security agency continued to conduct surveillance activities against the opposition. The original model of ministerial authorisation was introduced as an outcome of the events that took place during the 'Budapest Watergate' as a general approach; however, while the model was superseded for surveillance measures taken for the investigation of specific crimes, the procedure for secret intelligence gathering driven by national security remained mostly the same. I would like to express my special thanks to the anonymous reviewer for this valuable comment.

[33] <https://www.ajbh.hu/en/web/ajbh-en/> accessed 2 May 2018.

III Domestic Context

1 Procedural Background – Constitutional Complaint in the Practice of the Constitutional Court of Hungary

Pursuant to the effective provisions of Act CLI of 2011 on the Constitutional Court, constitutional complaint procedures have three different types in Hungary. As a common factor, these procedures have a concrete character, as all of them shall be used in cases where the complainant is personally concerned by the violation of fundamental rights enshrined in the Fundamental Law of Hungary.

Under Section 26 (1) a normative constitutional complaint might be launched when the violation of fundamental rights happened due to the application of a legal regulation in a particular judicial procedure in a way contrary to the Fundamental Law, targeting the legal regulation itself.

By an individual complaint regulated by Section 27, not the norm, but the interpretation of the legal regulation might be challenged, as the judicial decisions contrary to the Fundamental Law can possibly be set aside by the Constitutional Court. Both complaints governed by Section 26 (1) and 27 have an indirect nature, as the violation of the fundamental right is transmitted by a judicial procedure.

In the present case, the situation was different. As an exception, Section 26 (2), by introducing the direct normative constitutional complaint procedure, provides remedy for cases where a violation of fundamental rights happens by the mere fact of the application or the entry into force of the particular legal regulation, which means that the constitutional complaint procedure is not preceded by any judicial proceedings. Mr. Szabó and Ms. Vissy founded their argumentation on Section 26 (2) in this atypical case, with the explicit intention of testing the commitment of the Constitutional Court in Hungary to protecting the rule of law.[34]

To comply with the admissibility criteria is usually not without some trouble, though. According to Section 52 (1) of the Act on the Constitutional Court, the petition shall contain an explicit request, which – besides other factors – requires the petitioner to certify the existence of the preconditions for the proceedings. To illustrate the difficulty of the task, it might be established that the majority of complaint proceedings result in the petition being dismissed, and even complaints launched on typical issues (e.g. concerning local taxes) rarely comply with this criteria.[35] Considering the case of *Szabó and Vissy,* this rule would have obliged the petitioners to verify whether the application or the entry into force of the regulation in question had subjected them personally to a violation of their rights, which was

[34] László Majtényi, Máté Szabó. Beatrix Vissy, 'Mit keres a Terrorelhárítási Központ a paplan alatt? (Egy alkotmánybírósági beadvány értelme)' (2012) 46 (26) Élet és Irodalom.

[35] Fruzsina Gárdos-Orosz, 'The Hungarian Constitutional Court in Transition – from Actio Popularis to Constitutional Complaint' (2012) 53 (4) Acta Juridica Hungarica 315.

practically impossible, as the Act on National Security explicitly prohibits notifying the subject about the surveillance conducted.[36]

Despite all the sinister omens and regardless of the fact that it was never proved if the applicants were subjects of secret intelligence gathering at all, their potential victim status was accepted by the Constitutional Court of Hungary based solely on the existence of the legislation. The petition was found admissible having regard to the 'special nature' of the measure in question, with particular reference to the case law of the ECtHR.[37]

As secret intelligence gathering not linked to the investigation of any particular crime might include any person without tangible restrictions, the Constitutional Court failed to identify the possible personal scope of application. This complicated situation, together with the circumstance that the law itself hindered the complainants from collecting information on whether they had ever been subjected to the measure in question, entailed that even the Constitutional Court agreed that to require the petitioners to justify their victim status would be deeply unfair.

2 Summary of the Decision of the Constitutional Court of Hungary

In its decision no. 32/2013. (XI. 22.) AB, the Constitutional Court of Hungary dismissed the major part of the constitutional complaint launched by the applicants, concerning the compliance of the relevant legal background of secret intelligence gathering with the Fundamental Law of Hungary. The constitutional complaint broadly aimed that surveillance activities conducted by the Counter Terrorism Centre should be secured by similar legal guarantees provided by the Act on Police, instead of the Act on National Security, which provides fewer concrete safeguards.

Within the confines of the complaint claiming the lack of safeguards during the different stages of surveillance, the Constitutional Court examined whether the authorisation of the minister is enough to provide effective guarantees to prevent violation of the right to privacy and the right to informational autonomy. The CC noted that secret intelligence gathering is state interference, a serious threat to fundamental rights, therefore that the process must be regulated under the law, the underlying legal norms must be clear and it must be subject to external control mechanisms.

According to the Constitutional Court, the relevant legal norms meet the requirement of clarity, sufficiently specifying the conditions of ordering and the circumstances of executing national security-related intelligence gathering. The most important part of the decision concerned the question of the powers provided for the minister related to authorisation. In this regard, the Constitutional Court set forth that the scope of national security-related tasks is much broader than the scope of activities attached to the investigation of particular crimes. These purposes cover combatting endeavours to commit an act of terrorism in the territory

[36] *1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról* (Act CXXV of 1995 on National Security) s 58 para (6).

[37] E.g. *Klass and Others v Germany*, no. 5029/71, 37-38, 6 September 1978, and *Hadzhiev v Bulgaria*, no. 22373/04, 38, 23 October 2012.

of Hungary and the protection of Hungarian nationals at risk in a foreign country. In a broader sense, the task is to secure the sovereignty and the lawful order of the State. The CC argued that the connected 'events of real life' are not examined for their criminal law relevance; therefore the existence of a link to a particular crime is not an utmost necessity. On the basis of this argument, the CC found that national security-related issues *cannot be compared* to secret intelligence gathering linked to investigating a particular crime. This incomparability stands for the question of authorisation as well. Without further explanation, the CC stated that the prevention and elimination of risks to national security are *decisions of a political nature* and therefore such decisions fall within the competence of the executive power, justifying the authorisation rights granted to the minister.

At this point, there was an aspect on which the CC agreed with the applicants. Finally, it has been laid down in the decision as a constitutional requirement that the decision of the minister ordering secret intelligence gathering must be supported by reasons. The underlying argument was that, in granting the authorisation, it is the minister who must weigh the interests of national security against the harm caused to the fundamental rights. Without proper reasoning then, after the decision has been made, the considerations behind balancing cannot be reviewed. This element matters from the perspective of the external control provided by the National Security Committee and the Commissioner for Fundamental Rights, as they may only evaluate the lawfulness of the authorisation activity of the minister if the decision contains a detailed statement of reasons. Evaluating the effectiveness of the powers provided within the frameworks of control for the Committee and the Commissioner, the Constitutional Court established that the scheme provided by the law is sufficient to guarantee respect for the right to privacy.

IV The ECtHR's Judgement in Light of the Court's Standard

Analysing the case law of the European Court of Human Rights in the context of secret intelligence gathering, among other judgements, *Klass and Others v Germany*, *Weber and Saravia v Germany*[38] and *Roman Zhakarov v Russia*[39] *are considered to be the main cornerstones. This selection of cases is also justified by the fact that, in Szabó and Vissy v Hungary, even the Court itself used these cases as points of orientation.*

The Court examines all the interferences into the private sphere of the contracting party's nationals on the basis of Article 8 of the European Convention on Human Rights. According to the Court, any interference can only be justified in this field if it is in accordance with the law, pursues one or more of the legitimate aims listed by the Convention and is necessary in a democratic society in order to achieve any such aim. Secret surveillance of citizens is tolerable only if strictly necessary for safeguarding democratic institutions.

[38] *Weber and Saravia v Germany*, no. 54934/00, 29 June 2006.
[39] *Roman Zhakarov v Russia* [GC], no. 47143/06, 4 December 2015.

While the ECtHR's standard definitely does not show us a clear trend, there are still some basic developments which the Court seems to follow more or less consistently. This core standard, is filtered down from the previously listed decisions, seems to be as follows:

a) Article 8 on the right to private and family life has the broadest possible personal scope of application. The Court holds that the mere fact that such intrusive measures exist is a menace to the private life of everyone who the measures might concern. No further evidence is needed to comply with the admissibility criteria, as the harm is caused by the menace itself, not the actual application of surveillance measures. This approach was echoed by the decision of the Hungarian CC as well.

b) All the limitations of rights under Article 8 shall be interpreted narrowly.

c) The legal framework in effect has to clarify at least the nature of the offences in question and provide a definition of the categories of people affected. The minimum criteria requires a limit to be set on the duration of the measure; details to be given of the procedure to be followed for examining, using and storing the data obtained; and the clarification of the precautions to be taken when transferring data and the circumstances in which the data must be destroyed.

d) The interference shall be foreseeable in an abstract sense, which means that the individual does not need to foresee when his communications are likely to be intercepted. The legal framework has to provide a possibility for being informed of the existence of such measures, which doesn't even require states to list the specific offences which may give rise to interception.

e) To justify effective necessity in a democratic society, the Court requires a substantive reasoning, but in fact it tends to accept almost any reason as a legitimate aim under the cloak of national security.

f) The effectiveness of external control mechanisms is to be evaluated as a whole. The ideal form of control is of a judicial nature, because judicial control offers the best guarantees of independence and proper procedure. Judicial control is required 'at least' as a last resort, but involving judges doesn't fulfil the criteria in itself. Judges must have sufficient powers to evaluate the reasonableness of the suspicion on which the order is based, and the proportionality and necessity of the measures taken as well. Other solutions comply with the standard if the authority holds a sufficiently independent status, their powers are effective, it has the competence to exercise effective control, and the control mechanism has a democratic character in general.

g) Notification of the subject of surveillance is desirable as soon as it can be carried out without jeopardising the purpose of the restriction, after the termination of the measure taken.

*With regard to Szabó and Vissy, R*izzo establishes[40] that the ECtHR substantially confirmed the results achieved with the existing case-law. However, he highlights that there might be

[40] Giuseppe Rizzo, 'Szabó and Vissy v Hungary: a step back?' (2016) available at Lexology: <http://www.lexology.com/library/detail.aspx?g=435b47eb-31a0-4240-b17a-27894e7fffd7> accessed 2 May 2018.

a difference in the standard set for surveillance by the Zhakarov judgement and the present case. While the Court held in *Szabó and Vissy* that the decision on the motion of surveillance measures shall be based on 'an individual suspicion regarding the target person'[41], the previous requirement of 'reasonable suspicion' introduced by the Zhakarov decision was a more advanced criteria.

Even so, in accordance with the standard, in *Szabó and Vissy* the Court assessed secret intelligence gathering as a process, distinguishing between the question of authorisation and *a posterior* control of secret surveillance activities, but requiring the effectiveness of the protection of fundamental rights on the whole. The ECtHR acknowledged the absence of judicial supervision as a central issue common to both stages of the intelligence gathering process. With respect to the broad scope of application of the measure in question, the Court made it clear that the authorisation rights provided for the minister are incapable of ensuring the requisite assessment of strict necessity, as this kind of supervision is eminently political. Such a political nature increases the risk of abusive measures. According to the case-law, involving a non-judicial institution in authorisation might also be compatible with the Convention, but it has to be ensured that such authorisation is independent from the executive power, and it needs a proper justification. The Court doesn't consider *ex ante* authorisation an absolute requirement, because extensive *post factum* judicial oversight may counterbalance any shortcomings of the authorisation. For the Court, in the particular case, oversight by a politically responsible member of the executive did not provide the necessary guarantees. The Court also established that the responsible parliamentary committee's procedure falls short of securing adequate public scrutiny, and there is no remedy granted by the existing procedures, as those who are the subjects of secret surveillance are kept unaware of it, even after the end of the surveillance itself.

According to the Court, virtually any person in Hungary might be subjected to secret surveillance. The legislation doesn't describe or specify the categories of possible targets, or the underlying situations. The Court wasn't convinced that the relevant legal regulations provide sufficiently precise, effective and comprehensive safeguards on the ordering and execution of secret intelligence gathering. In sum, the ordering happens based on the decision of the executive power, without the assessment of strict necessity, and no effective remedial measures are provided at all.

V Conclusions

According to the fragments of the case law summarised above, there are at least three factors which might be identified as anomalous, considering the required level of fundamental rights protection provided by the ECtHR's standard and the Hungarian one.

[41] *Szabó and Vissy v Hungary*, 71.

a) The required nature of control

According to the ECtHR, political control of secret surveillance activities can only be considered as a sufficient safeguard if certain requirements are met. If the control is exclusively political, with no legal control mechanisms available as counterbalance, the level of clarity required for the relevant legal norms is increased. This seems a fundamental difference between the assessment of the ECtHR and the Constitutional Court, as the CC acknowledged the political nature of authorisation as a natural consequence of the political nature of the measure itself. Moreover, it could be added that not just the authorising decision but also the *a posterior* control conducted by the parliamentary committee has a political character, despite the fact that the task is to balance fundamental rights, which has an indisputable legal nature.

b) The meaning of 'external'

As the ECtHR established, control is only external if it is provided by a body independent of the executive power. The required level of independence was not evaluated by the Constitutional Court, but the ECtHR laid down that it is the judiciary that offers the broadest spectrum of guarantees in this field.

c) What 'effectiveness' stands for in practice

In the ECtHR's interpretation, effectiveness is the question of powers provided for the body involved in control. The key factor in providing effectiveness is publicity – legal remedies might only be effective if the subject is notified of the measures taken, at least afterwards, when providing information no longer represents a risk to national security. Similarly to the required nature of control, the CC also considered the lack of notification as a natural consequence flowing from the character of secret intelligence gathering, which obviously indicates a great gap between what the CC and what the ECtHR considers as an effective legal remedy.

The different institutional and procedural considerations listed above are at least those that the legislator should keep in mind when amending the underlying provisions to move the Hungarian standard towards the majority of Europe. Unfortunately, at this point some serious doubts need to be shared.

VI Doubts

Shortly after the autumn legislative schedule[42] of the National Assembly of Hungary was published, a new draft bill came out from the Ministry of Interior, aiming to re-structure the legislative framework of national security driven secret intelligence gathering in light of

[42] <http://www.parlament.hu/documents/10181/56621/tvalkpr_2017osz.pdf/3b362b76-01b0-426b-81b8-e5d8eb2cc3b6> accessed 2 May 2018.

the Strasbourg standard.[43] Even if all the rumours and press interviews available suggest that the draft bill in its present form will not be able to gain the required two-thirds majority, it is still worth having a look at the newly developed model to examine how the standard is currently understood.

According to the draft bill, it would be still the Minister of Justice who would authorise the application of surveillance measures, but his decision would be exposed to the ex-post review of the National Authority for Data Protection and Freedom of Information[44] within about a week. After the decision made by the Minister, the decision would be sent to the Authority within 48 hours, which would examine the decision within another 72 hours and send back the result of the review to the Ministry within further 48 hours at maximum. In the event of unlawful surveillance, the Authority would be entitled to terminate the measure taken, otherwise it would approve the decision of the Minister. The draft bill makes an attempt to clarify the possible personal scope of application, and introduces a remedial action called 'surveillance complaint', which could also be filed to the Data Protection Authority.

It is clear even for the very first glance that the requirements of the Strasbourg standard are a long way from being met by the draft.

a) The nature of authorisation would still be political. Even if a legal element (the approval of the Data Protection Authority) is introduced, this legal control – as a main rule – is only an ex-post control, which means that in practice, surveillance measures could still be undisturbedly taken for a whole week without any control outside the executive power. As an undeniable stride, the draft bill made significant progression in specifying the conditions of application, which could be a factor considered to be in harmony with the requirements. However, as with all legal norms which require balancing, these provisions will gain their true meaning in the course of their interpretation. That would make it immensely important to involve the independent judiciary in the process.

b) While the approval of the Data Protection Authority is external in the sense that the Authority is an autonomous administrative organ, the level of independence is far from the guarantees offered by the judiciary. Judicial control would not be part of the mechanism at any phase of the surveillance, and no justification explains the reasons.

c) The requirement of effectiveness would still not be fulfilled, as the 'surveillance complaint' would be introduced for persons who already believed they were subjected to intelligence gathering, while the draft bill remains silent about compulsory subsequent notification.

The title referred to a 'low threshold', reminding us that the standard of the ECtHR is self-evidently a minimum standard, still far from what we could call ideal. A gap was demonstrated between the actual trends in the literature and the approach of the Strasbourg Court, and moreover, another gap seems to have opened between Europe and Hungary as well. Based on the above, it truly seems that, for Hungary, even this low threshold currently seems too high to reach.

---

[43] <http://www.kormany.hu/download/8/d5/21000/Nbtv-Infotv%20m%C3%B3dos%C3%ADt%C3%A1s%20Normasz%C3%B6veg%2Bindokol%C3%A1s.pdf#!DocumentBrowse> accessed 2 May 2018.

[44] Hereinafter the Authority or the Data Protection Authority.