Security Sector Reform (SSR) in Practice in Europe and Central Asia – No. 2

DCAF Geneva Centre for Security Sector Governance

INSIGHTS AND LESSONS LEARNED FROM A SLOVENIAN JUDGE'S EXPERIENCE IN AUTHORIZING SECRET SURVEILLANCE

By Aleš Zalar

About DCAF

The Geneva Centre for Security Sector Governance (DCAF) promotes good governance and reform of the security sector. The Centre conducts research on good practices, encourages the development of appropriate norms at the national and international levels, makes policy recommendations and provides in-country advice and assistance programmes. DCAF's partners include governments, parliaments, civil society, international organisations and the range of security sector services, including the military, police, judiciary, intelligence agencies, and border security services.

Visit us at www.dcaf.ch

About the Series

The "SSR in practice in Europe and Central Asia" series comprises case studies in which security and justice sector practitioners reflect on experiences and offer personal insights about implementing reform in security sector institutions in transition environments, with a particular focus on the Western Balkans, Eastern Europe, the South Caucasus, and Central Asia. The papers provide insight into challenges and opportunities within security sector reform processes and address interests of practitioners, policy-makers, and researchers alike.

About the Author

Mr. Aleš Zalar served as the president of the District Court of Ljubljana, the largest court in Slovenia, for 16 years. Through his personal commitment to the rule of law and human rights standards, Mr. Zalar played an invaluable role in standardizing judicial supervision of the intelligence and security sectors in Slovenia. As the only judge authorized to exercise judicial control of surveillance measures, Mr. Zalar interpreted existing laws establishing legal standards in warrant authorisation and review, creating a judicial practice that fosters high levels of accountability in the work of intelligence and security agencies. During his tenure, the District Court of Ljubljana earned special recognition from the Council of Europe and the European Commission. In 2003, Mr. Zalar served on the group of legal experts who drafted the Slovenian law standardizing parliamentary oversight over intelligence and security agencies. Beyond the Slovenian system, Mr. Zalar has shared his experience with peers across Europe, advising fourteen European governments on topics spanning judicial independence and efficiency, combating corruption, alternative dispute settlement. Currently, Mr. Zalar is the President of the European Centre for Dispute Resolution and is actively supporting the DCAF Justice and Security Programme as senior justice consultant.

The views and opinions expressed in this paper are exclusively those of the author and do not necessarily reflect the official policy or position of DCAF, or the Government of Slovenia.

Acknowledgements

We would like to thank the members of the DCAF ECA editorial board for their dedication and the time they devoted to review this series: Teodora Fuior for providing feedback and comments to the author, Jennia Jin, Chloe Rudnicki and Krista Krien for their diligent editorial support.

Publisher

Geneva Centre for Security Sector
Governance (DCAF)

Maison de la Paix
Chemin Eugène-Rigot 2E;
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch

Insights and Lessons Learned from a Slovenian Judge's Experience in Authorizing Secret Surveillance

By Aleš Zalar

Rationale of judicial independence

Since 1978, when the European Court for Human Rights (ECHR) decided in the landmark case *Klass and others v. Germany*[1], it is an established legal standard that secret surveillance should be subject to an effective control, preferably assured by the judicial branch. The judiciary offers the best guarantees of independence, impartiality, and proper procedure. Judicial independence is paramount in this field; secret surveillance interferes with fundamental human rights, abuse is potentially easy, and could have harmful consequences for the whole democratic society[2].

Judicial independence is not a privilege of judges but a right of citizens. Both the organizational and individual judicial independence are of key importance, a "conditio sine qua non" for a fair judicial decision-making on secret surveillance measures. Organizational independence ensures that a judge can decide cases without restrictions, improper influence, inducements, pressures, threats, interference, whether direct or indirect, originating from any quarter or for any reason. Individual independence, as a state of mind, serves to guarantee judicial impartiality. It means that a judge is deciding a case without favour or fear.

Putting the principle of judicial independence into effect is a continuous challenge for all three branches of government (legislative, executive, and judicial) but also for every individual judges authorized to issue judicial warrants on intrusive methods of information collection (IMIC) due to deter threats to national security, or when ordering special investigative measures (SIM) to collect evidence for prosecuting serious crime. Courts and judges are in a difficult position when exercising judicial *ex-ante* authorization of IMIC and SIM. It is a daily struggle to perform with impartiality in an environment defined by competing facts, varying interpretations of laws, and wide discretionary powers. Besides, judges must deal with legal ambiguity and loopholes, secrecy of operations, files and hearings, limited access to relevant information and evidence, including their sources, lack of procedural competence, considerations that national security policy elements outweigh the adjudicative ones, difficulties in distinguishing between intelligence and counter-intelligence activity and overlapping of national security with crime prevention.

Looking back on my professional history concerning IMIC and SIM, I realize that there are several reasons as to why my judicial position has been somehow unique and important to the development of applicable principles and standards when authorizing IMIC and SIM.

Democratic changes

Until 1991, Slovenia was a federal republic of the former State of Yugoslavia. Until this time, the authority to invoke national security or criminal policy considerations to justify ordering restrictions of human rights through secret IMIC and SIM was in the hands of executive, not of the judiciary. Secret surveillance measures were neither regulated by the constitution nor by the statutory law, but by governmental regulations. The minister for Home Affairs was authorized to issue warrants for IMIC and SIM upon the proposal of the Security intelligence service or the criminal law enforcement service. Both services were organizational units within the Ministry for Home Affairs.

From the perspective of the standards as developed by the ECtHR, it was obvious that the minister for Home Affairs did not enjoy any independence from the executive. In fact, he was an integral part of the executive. Hence, it was not the influence of the emerging jurisprudence of the ECtHR that caused gradual

1 Judgement of the ECHR, Klass and others v. Germany, from 6th September 1978, Serie A, No. 28

2 Judgement of the ECHR in a case Kennedy v. UK from 18th May 2010, No. 26839/05

systemic regulatory changes concerning secret surveillance in Slovenia, but the reform process started as part of internal overall democratic transformation of the country.

In September 1989, the Slovenian parliament adopted a series of 81 amendments to the 1974 Constitution, which, for the very first time, empowered courts with ex-ante authorization for secret surveillance through interception of communications (telephone tapping, control of letters or other means of communication).

Following the constitutional amendments, the Slovenian parliament adopted and, on 1 June 1991, enacted amendments to the Law on Home Affairs and prescribed some general conditions for secret surveillance measures. Judicial warrants could be issued upon the proposal of the minister for Home Affairs. The law, however, was silent as to which court or courts should have jurisdiction for decision-making in these cases.

It was at this juncture that my judicial experience with IMIC and SIM began.

Lost in a desert

The turbulent times triggered by democratic reform processes did not spare the judiciary. In spring 1991, the president of the Basic Court in Ljubljana, also member of the Judicial Council, resigned because of his disagreement with the minister of Justice, ex officio member of the Judicial Council, concerning a request for dismissal of the president of the Supreme Court because of her past political engagement.

In late May 1991, I got a telephone call from the president of the Supreme Court that I should urgently meet with her. At that time, I served as a young judge (29 years old) and president of the County Court in Domžale, a small town near Ljubljana. At the meeting, I was asked to become the acting, temporary president of the Basic court in Ljubljana, which was and still is the largest court in the country, with over 100 sitting judges and 450 court staff. There were several reasons as to why she asked me to take over such an important position within the judiciary. Despite my age, I had an extensive experience with court management issues, as I served as a court administrator of the Ljubljana Basic Court two years before I became a judge; my superior then, the president of Court, resigned. It was therefore considered that I was well acquainted with the overall situation and challenges of the court. Besides, I successfully managed the County Court in Domžale as the president of the Court, and I was untainted by previous regime and political circles of power. Many judges at that time were members of the Communist party while I refused to join. Senior judges were reluctant to take such responsibility in the pre-war political context.

Once the president of the Supreme Court persuaded me to accept her proposal, she informed me that I would also be the only judge in the country with exclusive jurisdiction over cases concerning secret surveillance measures. The Supreme Court feared that it might be detrimental for its reputation to deal with such sensitive matters.

The Minister of Justice issued a classified order in writing determining the jurisdiction, concentrated on one judge – the president of the Basic court in Ljubljana – in order to ensure specialization and to reduce risks for national security; these would have been higher if a wider circle of judges had access to classified intelligence.

Thus, on 1 June 1991, I became the acting president of the Basic Court in Ljubljana. On the very same day, for the first time in the history of Slovenia's judiciary, I started exercising court jurisdiction in secret surveillance measures concerning interception and recording of communications in order to prevent threats to national security as well as for the purpose of all criminal proceedings at Slovenian courts. Since there was absolutely no previous domestic judicial case-law in these matters, I relied solely on standards established by judgements of the European Court for Human Rights. Moreover, there was no available and accessible domestic, electronic database of translated judgements yet. Fortunately, my English was good enough that I could search for relevant judgements of the ECtHR in its database. Nevertheless, at the beginning, I felt like a man lost in a desert. Due to the highest level of secrecy, there was no chance of consulting fellow judges to discuss the open legal issues, which is an established practice in other court cases. The fact that I was the only judge in the country authorized to issue judicial warrants on secret surveillance of communications automatically incurred the risk of considering such a role as incestuous. When you spend your full judicial time in the isolated world of security and intelligence, you could gradually lose the necessary awareness of the suspect's rights. I was aware of this risk.

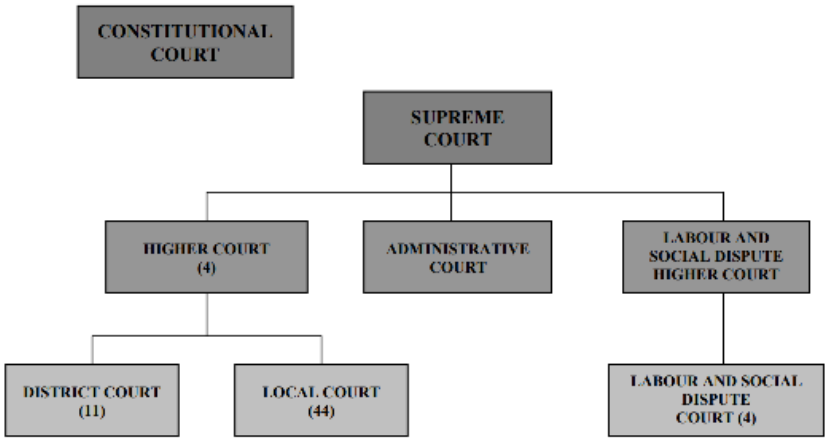


Figure 1. Organisation Chart of Slovenia Justice System[3]

Figure 2. 11 Districts of the Slovenia Justice System[4]

The war

Less than a month after I took office as the acting president of the Basic Court in Ljubljana, the ten-day Slovenian war for independence began, followed by Slovenia's declaration of independence from Yugoslavia. The war started on 27 June 1991.

The national security of the newly born state was under serious military threats. Yet, I did not consider this direct, imminent threat to territorial integrity as a "carte blanche" for rubber stamping, routine authorization of judicial warrants against targeted individuals, mostly commanders of the Yugoslav People's Army in Slovenia.

Despite a significant increase in the number of applications for IMIC during and some time after the war for independence, I adhered to **the Emerson's principles of judicial examination of national security**, inter alia, presumption in favour of individual rights, burden of proof rested on the applicant (minister for home affairs), direct, immediate, grave and specific harm to national security must have been shown, the restriction sought by the minister had to be confined to the narrowest possible constraint, necessary to achieve the goal, and I viewed claims of injury to national security with healthy scepticism. I believed that even the war time should not be an excuse for sacrificing rule of law, human rights, and democracy on the grounds of defending them. Everything we fought for would be lost.

Despite national security urgency, the Slovenian law did not envisage a possibility to deliver the so-called

3 CEPEJ - Organisation of the Judicial System of the Republic of Slovenia
4 CEPEJ - Organisation of the Judicial System of the Republic of Slovenia

"telephone justice" by oral approval of an orally proposed warrant for secret surveillance. Judges in some jurisdictions (e.g. in Austria), where such urgent oral authorization is allowed upon oral application by a prosecutor, are exposed to a certain risk: once they issue an oral judicial warrant, they must defend their decision even when ex-post written application for judicial warrant does not provide a sufficiently reasonable basis in facts to justify danger to national security.

I consider the time of the war for independence as the most difficult time in my entire judicial career. I was a judge on duty 24 hours per day. Security-intelligence services provided me with armed security agents who escorted and transported me from the Court to my home every night and back to the office in the morning to ensure my physical security and safety during the war. Should the President of the Presidency of Slovenia have declared a state of emergency, it was envisaged that I would have been appointed as President of an extraordinary military court with a seat at a secret location. Fortunately, this never happened.

I think that the lessons learnt from these exceptional circumstances positively influenced my competence and strengthened my personal independence as a judge.

The telephone tapping affair

National security can be a source of tension between the governing party or parties and the political opposition, or between political players and the staff of security or intelligence agencies. Switzerland, Sweden, Austria, and other Council of Europe countries already experienced cases of abuse of intercepted communications for inappropriate purposes. Slovenia is no exception.

It was more my sixth sense than anything else that helped me discover an attempt by the security-intelligence service to mislead me with an application for a judicial warrant for interception of communications, signed by the director of that agency. There was nothing in the standard explanation of reasons as to why the targeted person should be a threat to national security that would draw my suspicion, except the fact that the address of the person was that of an office on a street opposite to the courthouse where I sat. The identity of the person was known. The dynamics and the types of activities of the suspect were described. Relevant reasons justifying the suspicion that specific harm to national security existed were well argued. The reliability of the source of information was not problematic. The probability that targeted communication would be used was high enough. But the building where the suspect was located was known to me: it was the siege of trade unions and a leading political party whose president was the Speaker of the Parliament. I made an unusual check and dialed the telephone number which was to be tapped, and the secretary of the president of the political party indeed answered my call.

I officially informed the Minister of Justice about a potential attempt of abuse of power by the director of the security-intelligence service. During extraordinary ex-post control of all issued warrants, it was found that the security-intelligence service also indirectly controlled the prime minister, because the telephone number of his personal bodyguard was tapped, and his official position was not revealed in the application for judicial warrant.

Some time later, the prime minister dismissed the director of the secret service from his office. This affair triggered a process of reorganization of the security-intelligence service.

A valuable lesson we all learnt from this case was that **not only prior (*ex ante*) but also *ex-post* judicial and parliamentary control and oversight should be introduced to reduce the risk of abuse of powers** by security and intelligence agencies and to sanction abuses and amend laws in order to prevent they repeat in the future.

Development of judicial practice: between applying and creating the law

The poor quality of the Slovenian law regulating secret surveillance measures required certain judicial courage to adopt and insist on basic legal standards. These standards were not prescribed by the domestic statutory law but were developed through judicial interpretation of the general constitutional principles of the rule of law[5] and the supremacy and direct application of ratified international conventions[6], in

5 Article 2 of the Constitution of the Republic of Slovenia
6 Article 8 of the Constitution of the Republic of Slovenia

particular the European Convention on Human Rights. In many court decisions on the applications for judicial warrants, I therefore referred directly to relevant ECtHR judgements.

Limit the duration of a warrant

No reliable conclusions could be drawn from the ECtHR case law as to the appropriate maximum duration of IMIC in national security matters; therefore, each state enjoys a wide margin of appreciation (discretion) when addressing this issue.

The Slovenian Law on Home Affairs was silent as to the maximum duration of secret surveillance measures; the only limitation prescribed was that a measure should be temporary. Thus, I established a judicial practice of issuing judicial warrants allowing a maximum duration of 3 months. This was meant as a safeguard against the overuse of lengthy, unchecked secret surveillance measures.

Review the implementation of a warrant and its results

Since applications for the extension of secret surveillance measures were frequent, I systematically included in judicial warrants the applicant's duty to provide the court with a written report on the implementation of the warrant with a time limit for the delivery of this report. An especially sensitive issue in national security cases was my insistence that, whenever appropriate, any application for an extension should be accompanied by a temporary access to recordings or transcripts of intercepted communications for my review as authorizing judge. T**he discretionary power of a judge means that, whenever the judge deems it appropriate, he/she may order certain conditions for the implementation of a judicial warrant as part of the procedure for examining, using, and storing data and information obtained by a warrant.** When I ordered access to the recordings and transcripts for the first time, the security-intelligence service rejected their delivery. Consequently, I refused the application for the extension of the IMIC. The outcome of this controversy could not have been other than a change of status-quo. The security-intelligence service accepted my request, provided me with recordings of intercepted communications, and this newly established legal standard was implemented in all subsequent cases. I managed to set a precedent proving that **judicial powers in practice are not less effective than legal powers written on paper**.

Beware the importance of factual information

Winston Churchill explained the role of security and intelligence agencies as follows: "They are the geese that laid the golden eggs and never cackled". A common feature of the applications for judicial warrants in national security cases is that they contain as little factual information as considered necessary by the applicant. This is the common approach because intelligence and security agencies are generally reluctant to expose sources of information or identities of staff to the court, considering the court as part of the outside world. Nevertheless, a standard burden of proof, set at the level of legitimate reasons to believe that a significant risk for national security exists or may occur in the future, rests on the applicant agency. There is no presumption that the reasons invoked by the applicant exist and are valid. Sometimes the applicant simply tried to embark on a fishing expedition to bring in information and it is commonly recognized that very often, the quality of such information is typically low. Without having sufficient factual information, a court cannot balance the interest for national security against the seriousness of interference with basic human rights, which is a key challenge[7]. Description of facts should allow the court to effectively assess the reliability of the source of information presented as a ground for suspicion that national security is or may be threatened. I always tried to insist on the presentation of concrete facts by the applicant, and such judicial practice had an obvious deterring effect to unmeritorious applications.

Foster the exchange of information with the Court by promoting innovative procedure

The source of information of intelligence and security agencies is often based upon exchange of such information with foreign counterparts upon condition to be kept classified. The de-classification process at the time when I served as a judge was not regulated. I have not considered secrecy itself as prima facie evidence of wrongdoing. However, judicial validation of provided information in such cases should not be based only upon a presumption of a good faith. The quality of presented second-hand evidence only in a form of a reference to the information, obtained by foreign intelligence agency, is undermined. Thus, I decided to introduce, without having any clear statutory ground as the basis, an **in-camera inspection – a confidential hearing at which an authorized official of the intelligence agency orally provided me with**

7 See the judgement of the ECHR in the case Janowiec and others v. Russia from 21th October 2013, No. 55508/07 and 29520/09

additional information, clarification, or explanation of facts. This procedural event has proven to be very helpful to both the applicant and me as a judge. During the in-camera inspection I could also see some classified documents presented by the intelligence agency official. The hearing was not recorded. Its minutes only stated when it was held, who attended, and the duration of the hearing.

To summarize, **in a state governed by the rule of law, judges determine what the law is and what the law says**. One might consider this as judicial activism, but as long as it is in favour of protecting human rights and has a basis in universally recognized minimum standards of human rights and fundamental freedoms, I believe it is appropriate.

Constitutional review and statutory law-making

Judicial independence and authorization of secret surveillance measures are a prerequisite of an effective control and a powerful safeguard against abuses of human rights; however, judicial authorization is not sufficient for deterring massive overuse of secret surveillance.

In 1994, Slovenia enacted a new Criminal Procedural Code (CPC), which regulated secret surveillance measures to prevent and combat serious crime. Investigative judges of 11 district courts became authorized to issue judicial warrants for SIM. Surprisingly, the CPC did not derogate the provisions of the Law on Home Affairs as concerns the SIM for the purpose of criminal proceedings. Therefore, a double regime, which ran in parallel to the already existing one, was established.

The law enforcement division of the Ministry for Home Affairs started applying for judicial warrants for SIM at investigative divisions of district courts, but not always. Occasionally, the Ministry for Home Affairs still applied for judicial warrants upon provisions of the Law on Home Affairs and in such a case, it was my responsibility to decide whether to grant the warrant.

Applicants soon began exploiting the above-described two possible tracks for obtaining a judicial warrant, because when the application for a judicial warrant was rejected by the investigative judge, the applicant filed the same application against the same suspect with the same justification to me as the president of District Court in Ljubljana. The problem of this inappropriate practice was that every case, which concerned SIM for the purpose of criminal proceedings, was (and still is) classified. In addition, there were different systems of registration of these cases in the court dockets. Consequently, I was never aware of cases which had already been ruled on by the investigative judges. This practice was, in fact, a specific way of *judge shopping* and represented an abuse of the system of legal remedies by the official authorities to the detriment of individuals.

When I discovered this manipulative practice in a pending case, by requiring a written assurance that the warrant application was not filed beforehand to any investigative judge, I decided to suspend the proceedings and filed the request for constitutional review of the relevant provisions of the Law on Home Affairs[8]. I justified the request for review of constitutionality by challenging the poor quality of the law. Any such law should provide guarantees against abuse and prescribe with clarity and specificity the duration for measures, grounds for ordering, and the nature, scope, and manner of limitations on human rights and freedoms.

The Constitutional court annulled the challenged provisions of the law and ordered that its decision should come into effect in 6 months after the day when it was published[9].

The political storm which followed the decision of the Constitutional Court led to the failure to implement the decision on time. Since the annulled legal provisions could cause a legal lacuna, a loophole which could result in absence of any statutory ground for judicial warrants in national security matters, I turned to the Constitutional Court again and, as a president of district court, suggested the extension of the deadline for the implementation of the Constitutional Court decision, aimed at not putting national security at any risk. The Constitutional Court extended the deadline for an additional 6 months[10] and before this deadline expired, the Parliament adopted the new Act on the Slovenian security-intelligence agency[11].

8 Article 156 of the Slovenian Constitution prescribes that a judge, who considers applicable law as contrary to the constitution, must suspend the decision-making proceedings and request the review of constitutionality of that law at the Constitutional court

9 Decision of the Constitutional court from 2nd.April 1998, U-I-158/95

10 Decision of the Constitutional court from 14th October 1998, U-I-158/95

11 Published in the Official Gazette No.23/99

My last contribution to the domestic systemic development of secret surveillance regulatory framework occurred in 2003 when I was invited by the Parliament to join the small group of legal experts entrusted to prepare first draft Law on parliamentary oversight on intelligence and security agencies. The Parliament unanimously adopted this law in the same wording as it was prepared by the expert group[12]. I consider this contribution to the secret surveillance regulatory framework to be an outstanding achievement.

THE PARLIAMENTARY CONTROL OF INTELLIGENCE AND SECURITY SERVICES ACT
April 2003 (Official Gazette of the RS, No. 26/03 – ZPNOVS)

Article 2

Control under the present act is exercised by the Commission for Control of Intelligence and Security Services (hereinafter: the Commission).

Article 10 (composition of the Commission)

(1) The Commission has at most nine members.

(2) The chairman, deputy chairman and members of the Commission are elected by the National Assembly by a majority vote of all deputies on the proposal of deputy groups.

(3) A member of the Commission who is absent can not be substituted for by another deputy.

Article 11 (manner of work of the Commission)

(1) The sessions of the Commission are closed to the public.

(2) On the proposal of its chairman or a deputy group the Commission may decide by a two-thirds majority vote of the members present that a session or part of a session will be public.

(3) The Commission may not take decisions at correspondence sessions.

Article 19 (report on the application of controlled measures)

(1) Every four months, and also additionally if necessary, the controlled intelligence service reports to the Commission on the application of controlled measures.

(2) The report on the application of controlled measures of the intelligence service ordered by court decision also includes the following data:

- the number of cases in which measures have been ordered;
- the number of persons against whom measures have been ordered;
- the number of persons against whom measures have been applied;
- the number of rejected proposals to order measures;
- the legal grounds for ordering measures in individual cases;
- the number and type of communication means controlled in individual cases;
- the time period for which individual measures have been ordered in individual cases;
- data on established irregularities in applying the measures in individual cases.

(3) The report on the ordering and application of controlled measures of the intelligence service which are not ordered by court decision contains, mutatis mutandis, the same data as specified in the preceding paragraph.

(4) The report from paragraphs (2) and (3) of this article also contains data on controlled measures that have not yet been concluded.

(5) The Commission may also request a detailed report on particular controlled measures.

12 Published in the Official Gazette No. 26/03

I consider the parliamentary control over security and intelligence services of key importance, and even as meaningful when concerning judicially ordered secret surveillance measures. There is a clear legal distinction between judicial and parliamentary powers in the way that the parliament cannot examine whether a judicial decision was correct or not. The classified status of judicial decisions and the narrow jurisdiction of courts and judges require additional safeguards to prevent massive overuse of secret surveillance measures and to resist temptations to issue judicial warrants based predominantly on a presumption of good faith.

Circumstances such as the war for independence or Slovenia's negotiations for joining the EU and NATO sometimes triggered dubious applications for judicial warrant on secret surveillance measures. Strong judicial courage, supported by the principle of judicial independence and the rule of law, was needed to turn down applications for such warrants. The burden of responsibility was high, and in such cases, it is good that individual judges know that he/she is not the only person who takes part in exercising checks and balances powers. Ex post parliamentary control matters as well.

Conclusions

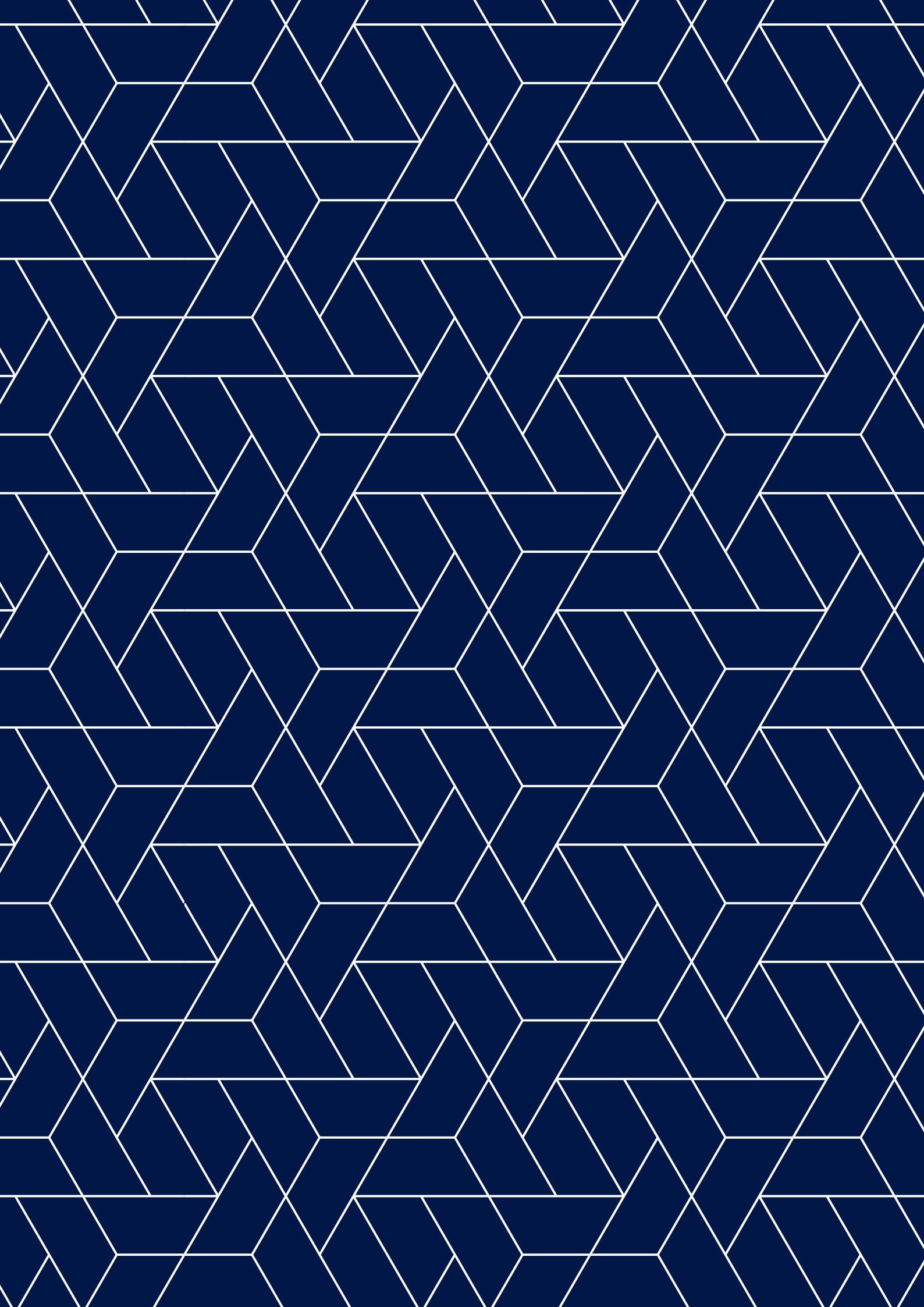
The main advantage of judicial supervision of security and intelligence agencies is that the public can be reassured that the letter and the spirit of the law, as interpreted by courts, will be applied. However, a challenge for judicial decision-making remains the very nature of security surveillance. An inherent feature of it is that surveillance usually comes at the very early stage of investigation and is of an exploratory nature. The suspicions will be often very loose at the time when the application for judicial warrant is to be filed[13].

To serve as an authorizing judge for security and intelligence surveillance, a judge must be given time to develop his/her experience and expertise regarding the nature and the sort of information or evidence that can and should be obtained from a secret surveillance operation. Judicial training is, of course, very important, but learning by doing is key.

My judicial time of adjudicating in secret surveillance matters was very long; I served in this capacity for 16 years. Today, I have the privilege to share my experience with judges all over the world. My usual advise to them is simple: Stay independent and courageous!

There is no uniform standard as to how much judicial intervention in the national security or criminal justice policy is appropriate, but the existing experience and practice of functioning democracies makes one thing clear: **judicial control over secret surveillance is, because of judicial independence and impartiality, the best guarantee for maintaining and developing our democracies**. This does not exclude considerations of who shall watch over judges as the watchmen, but judicial accountability is another challenging issue beyond the purpose of this article.

13 See more about advantages and disadvantages with judicial controls in I.Cameron: National Security and the European Convention on Human Rights, Kluwer Law International, 2000, page 157-161



DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva