Operative-investigative work in Georgia: a critical analysis in the light of international human rights standards

Ralf Alleweldt
Professor of Law, Brandenburg State Police University, Oranienburg, Germany

November 2019

Introduction

It is a fundamental responsibility of any government to protect citizens and society from criminal acts. Accordingly, the laws usually regulate the powers to investigate crimes that have already been committed, as well as to prevent criminal acts that are in the course of being committed, prepared or planned. In Georgia, in addition to the investigatory powers as laid down in the Code of Criminal Procedure and the preventive powers of the police as laid down in the Law on the Police, the "Law on Operative-Investigative Activities" provides a number of government authorities with the power to use (mainly) covert methods in order to "identify, put an end to and prevent a crime or any other unlawful act" (Article 3). The present paper undertakes to analyse this Law in the light of international standards on crime prevention and detection, as they have been developed, in particular in the field of human rights law, during the last decades.

Part 1. International standards on crime prevention and detection

I. Crime prevention

The concept of "crime prevention" may be used in (at least) two different meanings: a more general meaning – prevention of crime as a matter of policy – and a more specific meaning: prevention of a particular criminal act.

1. Prevention of crime as a general responsibility of the state

The term "prevention of crime" is sometimes used in a general sense as comprising all state activity aimed at reducing the crime rate, usually carried out in various sectors and including measures of social policy, education towards pro-social behaviour, and support the well-being of people in general. This is the meaning given to crime prevention, for example, in the context of United Nations activities like the "Guidelines on the prevention of crime" adopted by the Economic and Social Council (ECOSOC) in 2002, which state

> "3. For the purposes of the present guidelines, 'crime prevention' comprises strategies and measures that seek to reduce the risk of crimes occurring, and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes. (…)"

and define, more specifically

> "6. Crime prevention encompasses a wide range of approaches, including those which:
> (a) Promote the well-being of people and encourage pro-social behaviour through social, economic, health and educational measures, with a particular emphasis on children and youth, and focus on the risk and protective factors associated with crime and victimization (prevention through social development or social crime prevention);
> (b) Change the conditions in neighbourhoods that influence offending, victimization and the insecurity that results from crime by building on the initiatives, expertise and commitment of community members (locally based crime prevention);
> (c) Prevent the occurrence of crimes by reducing opportunities, increasing risks of being apprehended and minimizing benefits, including through environmental design, and by providing assistance and information to potential and actual victims (situational crime prevention);
> (d) Prevent recidivism by assisting in the social reintegration of offenders and other preventive mechanisms (reintegration programmes)."[1]

[1] United Nations Guidelines on Crime Prevention, ECOSOC Resolution 2002/13, 24 June 2002, Annex. Printed in United Nations Office on Drugs and Crime (UNODC) (ed.), Compendium of United Nations standards and norms in

Prevention of crime in this wide, general sense may be considered to be an extremely important task of any government, having a high potential to reduce all kinds of criminal and other anti-social behaviour. Accordingly, crime prevention is certainly an important aspect of good governance. As may be seen, for example from the UNODC Compendium of UN standards and norms in crime prevention and criminal justice, quite a number of international standards exist in this respect. From a legal point of view, however, these standards contain very few hard legal rules obliging states to pursue a certain policy. States may be obliged to pursue a general policy of crime prevention, but legally they certainly have a very large room for manoeuvring. So the scope and extent of a particular state's activities in general crime prevention are, in essence, a matter of criminal and social policy, while international law contains only very few requirements in this respect.

2. Prevention of specific criminal acts

"Crime prevention" in the second possible meaning is about the prevention of specific criminal acts which are already underway or planned. It is a typical task of police forces not only to contribute to the investigation and prosecution of criminal offences already committed, but also to prevent such offences from happening, as far as possible. Each time the police learns about a crime that is about to be committed, it has the power – and indeed, in serious cases often the obligation – to stop the perpetrator and prevent the offence from being carried out. Prevention of crime as a general policy, within the first meaning, is usually aimed at creating a framework for reducing the crime rate, including various forms of support given to citizens and communities. In contrast, the second form – stopping the persons suspected of a criminal activity – usually constitutes, or involves, an interference with their human rights.

3. Operative-investigative activities as measures aimed at detecting and preventing specific criminal acts

For the purposes of the present paper, "crime prevention" is used in the second, more specific meaning. While operative-investigative activities under Georgian law may contribute to the prevention of crime in a general sense, their principal purpose is to prevent or detect specific acts of a criminal or other unlawful nature. This is underlined by the wording of Article 3 of the Law

---

crime prevention and criminal justice, New York 2016.
https://www.unodc.org/pdf/criminal_justice/Compendium_UN_Standards_and_Norms_CP_and_CJ_English.pdf.

on Operative-Investigative Activities which states that the objectives of such activities are, inter alia, to "identify, put an end to and prevent a crime or any other unlawful act".
The legal issues connected with operative-investigative activities often concern their compatibility with the human rights of the citizens subjected to such activities.

II. Operative-investigative activities

1. The lack of an international definition

Operative-investigative activities are a concept of Georgian law and some other national legal orders, having their roots basically in the legal order of the Soviet Union. It is not a concept of international law. There is no definition of such activities in the international legal order. There are no rules in international law, nor other international standards, which deal with "operative-investigative activities" as such, using exactly these words. Thus it is not possible to give a general statement as to whether operative-investigative activities are compatible with international standards.

However, operative-investigative activities comprise several state activities which may interfere with the human rights of a person. Naturally, all state activities must comply with international law, in particular with international human rights standards. Accordingly, it is necessary for the purposes of this paper:

1. to clarify which particular operative-investigative activities exist under Georgian law,

2. to identify the international standards applicable to each of these measures, especially as regards crime detection and prevention,

3. and to conduct a legal analysis as to whether and under which conditions operative-investigative activities are compatible with these standards.

But before we can conduct such an analysis, we need a clear understanding of what exactly are operative-investigative activities under Georgian law, and for which purposes they may be used.

2. Objectives of operative-investigative activities and their relevance for the prevention or detection of crime

Operative investigative activity in Georgia is "a system of measures performed (…) by overt or covert methods (…) in order to protect human rights and freedoms, the rights of legal persons, and public security against criminal and other unlawful encroachments." (Article 1 of the Law on Operative-Investigative Activities). Such measures are designed to combat criminal (and other unlawful) activity, and, according to Article 3 of the Law, their most important objectives are to:

> a) identify, put an end to and prevent a crime or any other unlawful act;
> b) identify a person who prepares, commits or who has committed a crime or other unlawf ul act;
> c) for the purpose of presenting him/her to a relevant state authority, locate a person who, despite having been summoned, fails to appear before an investigation or a court; to search for an accused or convicted person and ensure their appearance before a relevant state authority (…);
> d) search for and identify the property lost due to criminal or other unlawful activity;
> e) search for a missing person;
> f) obtain necessary facts in a criminal case;
> g) identify (name, surname, age, citizenship) the perpetrator of a crime or of any other unl awful act;
> h) provide information and analytical support for the management of prison facilities.

With the possible exceptions of categories e) and h) all these objectives are related to preventing, detecting or putting an end to criminal and other unlawful activity. Operative-investigative activities may in particular be conducted when

- there are indications that a crime might be committed in the future (prevention),
- there might be unknown ongoing criminal activity (detection), or
- a crime may have been committed in the past, but an investigation has not yet been initiated.

Operative-investigative activities may come into play especially at a point in time when a criminal investigation – which has to be initiated once "information of a crime" has been received by an investigator or prosecutor (Article 100, 101 of the Criminal Procedure Code of Georgia) – has not yet started.

In sum, the most important objectives of operative-investigative activities are the prevention and detection of crimes and other unlawful acts. This paper will concentrate on these objectives of operative-investigative activities.

3. The covert nature of operative-investigative activities

As indicated above, operative-investigative activities may be carried out overtly or covertly. When carried out covertly, operative-investigative activities are likely to be most effective, and at the same time, are particularly intensively interfering with the human rights of individual persons. Therefore this paper will concentrate on the analysis of covert activities in the light of international human rights standards and practices.

III. Applicable international standards

1. Standards for criminal investigations

As regards criminal investigations, the most important human right is the right to a fair trial, as laid down in Article 6 of the European Convention on Human Rights. This right is applicable once a person is "charged with a criminal offence" within the meaning of Article 6 para. 1, i.e. once the person has been given "the official notification (…) of an allegation that he has committed a criminal offence"[2]. Accordingly, this right is applicable during any criminal investigation, but often not during operative-investigative activities since they do not necessarily relate to a crime that has already been committed.

2. A standard applicable to all police activity: the right to respect for private life

A human right which is applicable to all operative-investigative activities, in contrast, is the right to respect for private life, as laid down in Article 8 of the Convention. This is the main human rights standard for covert activities directed at the prevention and detection of crime.

The detailed requirements of Article 8 for operative-investigative activities will be described in following sections of this paper. These requirements are laid down in the case-law of the European Court of Human Rights.

3. Operative-investigative activities and Special Investigative Techniques. The Council of Europe Recommendation

[2] European Court of Human Rights, Deweer v. Belgium, 27 February 1980, §§ 42, 46; Eckle v. Germany, 15 July 1982, § 73. All judgments of the Court are available at: https://hudoc.echr.coe.int.

In addition to these considerations, it should be noted that the Committee of Ministers of the Council of Europe has issued, in 2017, a Recommendation concerning the use of "Special Investigation Techniques" in a criminal context. Although "Special Investigate Techniques" are not identical to "operative-investigative activities", these concepts overlap considerably so that the Recommendation is applicable to operative-investigative activities under Georgian law to a large extent.

According to the Recommendation, special investigation techniques, being of a covert nature, mean "techniques applied by the competent authorities in the context of criminal investigations for the purpose of preventing, detecting, investigating, prosecuting and suppressing serious crimes, aiming at gathering information in such a way as not to alert the target persons".[3]

It should first be noted that the Recommendation comprises covert techniques applied for preventing and detecting crimes. Accordingly, it applies not only to investigations of past offences, but also to covert operative-investigative activities in a criminal context, i.e. exactly those activities under consideration in the present paper.

Second, according to the Explanatory Memorandum of the Recommendation, the definition of Special Investigative Techniques may include: "undercover operations (including covert investigations); front store operations (e.g. undercover company); informants; controlled delivery; observation (including cross-border observation); electronic surveillance of specific targets; interception of communications; cross-border (hot) pursuits; pseudo-purchases or other 'pseudo-offences', covert monitoring of financial transactions and web traffic as they are defined in national legislation."[4]

It will be recalled that according to Article 7 para. 2 of the Georgian Law on Operative-Investigative Activities, the competent bodies may (overtly or) covertly:

a) interview a person;
b) collect information and conduct surveillance;
c) carry out a test purchase;
d) carry out a controlled delivery;
e) examine objects and documents;

[3] Council of Europe, Committee of Ministers, Recommendation CM/Rec(2017)6 of 5 July 2017 on "special investigation techniques" in relation to serious crimes including acts of terrorism, Appendix, § 2 and Preamble.

[4] Council of Europe, Committee of Experts on Terrorism (CODEXTER), Recommendation CM/Rec(2017)6, Explanatory Memorandum, CM(2017)58-addfinal, § 32.

f) identify a person;
g) censor the correspondence of an arrested, detained and convicted person;
h) obtain electronic communication identification data;
j) infiltrate a secret collaborator or an operative into a criminal group in a prescribed manner;
k) set up an undercover organisation in a prescribed manner;
l) monitor Internet communications by observing and participating in open and closed Internet communications in the global information network (Internet), and creating situations of the illegal obtaining of computer data in order to identify a perpetrator.

It may immediately be seen that the operative-investigative activities mentioned in paragraphs b) (surveillance), c, d, g, h, j, k, and l are at the same time "Special Investigative Techniques" within the meaning of the Recommendation. The same is true of the activities a) (interview a person) and b) (collecting information on a particular person) if these activities are conducted by a police informer.

It follows that the Recommendation is an important international standard applicable to operative-investigative activities under Georgian law. While it is formally of a non-binding character, it reflects the common views of the all governments of the Council of Europe member states on many of such activities. On the following pages, reference will be made to the Recommendation repeatedly.

It should be noted that, according to the Recommendation, governments have the power to use Special Investigative Techniques ("SIT") – subject to certain limits – but they are not under obligation to introduce or use them. Although the Recommendation provides in § 4 that "Member States should take appropriate legislative measures to allow, in accordance with Chapter I, the use of special investigation techniques with a view to making them available to their competent authorities to the extent that this is necessary in a democratic society and indispensible for efficient criminal investigation and prosecution", the Explanatory Memorandum (§ 43) makes clear that "paragraph 4 should not be interpreted as an obligation on member States to introduce additional SIT. The SIT that should be available depend on what is considered appropriate by national legislative authorities."[5]

Part 2. The Georgian Law on Operative-Investigative Activities

[5] Council of Europe, Committee of Experts on Terrorism (CODEXTER), Recommendation CM/Rec(2017)6, Explanatory Memorandum, CM(2017)58-addfinal, § 43.

and the right to respect for private life

The aim of this chapter is to analyse under which conditions operative-investigative activities are compatible with the right to respect for private life as guaranteed, e.g., under Article 8 of the European Convention on Human Rights, in particular if they are carried out covertly.

Article 8 of the Convention 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.

Accordingly, it must be determined whether, and which, operative-investigative activities, as described in the previous section, qualify as interferences in the human right to respect for private life, what are the conditions for lawful interferences with this right, and whether operative-investigative activities under Georgian law satisfy these conditions.[6]

I. Operative-investigate activities as interferences with the right to private life and to correspondence

The European Court of Human Rights considers private life to be "a broad concept incapable of exhaustive definition"[7]. It may “embrace multiple aspects of the person’s physical and social identity”[8]. In essence, cases concerning private life may be grouped into three categories: they may affect a person's (1) integrity, (2) identity and (3) privacy. Operative-investigative activities may touch the right to privacy in this sense.

---

[6] The following case law description is partly inspired by European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, 2018.

[7] See, for example, European Court of Human Rights, Niemetz v. Germany, 16 December 1992, § 29; Peck v. United Kingdom, 28 January 2003, § 57.

[8] European Court of Human Rights, S. and Marper v. United Kingdom [GC], 4 December 2008, § 66.

The Court has held that with respect to surveillance and the collection of private data by agents of the State, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8 § 1 of the Convention.[9] Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged[10]. In a case where the police collected information about journeys made by a particular citizen, the Court held that the collection and storing of that data amounted to an interference with private life.[11] "Private life" encompasses also, for example, the data on the telephone numbers dialled, information relating to telephone, email and Internet usage and information about an applicant's business relations.[12] Files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[13]

As to the definition of private or personal data, the Court has advocated a broad interpretation, corresponding with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2).[14]

It follows that whenever the government collects data relating to specific persons, it interferes with their private life. This is in particular true when the state approaches citizens, directly or indirectly, for the purpose of collecting data in order to investigate, detect or prevent crime, and if the data are collected covertly, as may be the case with operative-investigative activities in Georgia.

---

[9] European Court of Human Rights, Shimovolos v. Russia, 21 June 2011, § 65; Amann v. Switzerland, 16 February 2000, § 70; Benedik v. Slovenia, 24 April 2018, § 103.

[10] European Court of Human Rights, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], 27 June 2017, § 137; Benedik v. Slovenia, 24 April 2018, § 103.

[11] European Court of Human Rights, Shimovolos v. Russia, 21 June 2011, § 65.

[12] See European Court of Human Rights, Malone v. United Kingdom, 2 August 1984, § 84; Copland v. United Kingdom, 3 April 2007, §§ 41, 42; Amann v. Switzerland, 16 February 2000, § 66.

[13] European Court of Human Rights, P.G. & J.H. v. United Kingdom, 25 September 2001, § 57.

[14] European Court of Human Rights, Amann v. Switzerland, 16 February 2000, § 65.

On the basis of these considerations, most operative-investigative activities, as laid down in Articl 7 para. 2 of the Law, constitute interferences in the right to private life. It is rather obvious that the state collects data about a person – regardless of whether it acts through an official state agent or by using an informant – if it

- interviews a person (a),
- collects information about a person (b)
- conducts surveillance of a person (b)
- examines objects and documents (c), at least if they relate to a information about a person,
- identifies a person (f)
- obtains electronic communication identification data[15] (h) or monitors Internet communications (l)

Certainly censorship of the correspondence of an arrested, detained or convicted person (g) is, apart from being an interference with the right to correspondence, also involving data collection about the person and thus an interference in the right to private life.

When the state carries out a test purchase (c) or a controlled delivery (d), it collects data as regards the activities of the involved persons. When the state infiltrates a secret collaborator or an operative in a group considered criminal (j), it collects data about the members of the group. Setting up an undercover organisation (k), as such, is not necessarily connected with collection of data about persons. But it may fairly be assumed that the establishment of such an organisation is not an end in itself, but it is designed, inter alia, to collect data about the activities of persons with a view to ascertaining whether such activities are criminal or not.

In sum, operative-investigative activities under Georgian law will usually involve an interference with the right to private life of the affected citizen(s) within the meaning of Article 8 of the Convention. Such activities may be very diverse as regards their character and intensity, and it will be easier to justify such a measure if it involves only a slight interference with the right to private life. Still, in any case an operative-investigative activity is only lawful if it is justified under the second paragraph of Article 8 of the Convention.

II. Justification of interferences with private life under the Convention

According to the text of the Convention (as well as the constant case-law of the Court), any

[15] European Court of Human Rights, Malone v. United Kingdom, 2 August 1984, § 84.

interference can only be justified under Article 8 para. 2 if it is

1. in accordance with the law,

2. pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers, namely
- national security,
- public safety,
- the economic well-being of the country,
- prevention of disorder or crime,
- protection of health or morals
- protection of the rights and freedoms of others,

3. is necessary in a democratic society in order to achieve any such aim.[16]

As to the second of these conditions, it is relatively easy to meet for governments. All measures designed to prosecute or prevent crime aim at least at the "prevention of disorder and crime", as well as at the protection of the rights and freedoms of others, or at preserving public safety or national security. Thus, usually the points at issue in Article 8 cases are whether state action is "in accordance with the law" and "necessary in a democratic society".

1. "In accordance with the law"

According to the well-established case-law of the European Court of Human Rights, the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the Rule of Law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects.[17]

Similarly, the Recommendation on Special Investigative Techniques provides:

[16] See, for example, European Court of Human Rights, Roman Zakharov v. Russia [GC], 4 December 2015, § 227; Kennedy v. United Kingdom, 18 May 2010, § 130.

[17] European Court of Human Rights, Roman Zakharov v. Russia [GC], 4 December 2015, § 228; Rotaru v. Romania [GC], 4 May 2000, § 52; S. and Marper v. United Kingdom [GC], 4 December 2008, § 95; Kennedy v. United Kingdom, 18 May 2010, § 151.

> 3. Member States should, in accordance with the requirements of the European Convention on Human Rights (ETS No. 5) and the relevant case law of the European Court of Human Rights, ensure that the circumstances in which, and the conditions under which, the competent authorities are empowered to resort to the use of special investigation techniques are provided for by law with sufficient clarity.
>
> 4. (…) Domestic legislation should afford adequate and effective guarantees against arbitrary and abusive practices, in particular with regards to the right to a fair trial, the right to respect for private and family life, including the right to protection of personal data, freedom of expression and communication, the right to an effective remedy, and protection of the right of property as enshrined respectively in Articles 6, 8, 10 and 13 of the Convention and in Article 1 of Protocol 1 to the Convention.
>
> 7. Special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared, by one or more particular persons or an as-yet-unidentified individual or group of individuals.[18]

a. Foreseeability in the context of the secret surveillance measures and the risk of arbitrariness

"Foreseeable" in this context cannot mean that individuals should be able to foresee when the authorities are likely to resort to secret surveillance so that they can adapt their conduct accordingly[19], since it is the very purpose of secret surveillance measures to acquire information which the affected persons would not give voluntarily to the state authorities. On the other hand, in a human rights perspective secret state measures interfering with citizens' rights carry particular risks. Since citizens may never learn that an interference with their rights has occurred, the risk that secret state measures are exercised arbitrarily is inherently higher than in other cases. Under the Rule of Law, "domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances and conditions under which public authorities are empowered to resort to any such measures"[20].

With regard to the secret surveillance of communications, including telephone tapping, the Court has considered that, since their practical implementation is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the Rule of Law for the discretion

[18] Committee of Ministers, Recommendation CM/Rec(2017)6, Appendix.

[19] Cf. European Court of Human Rights, Roman Zakhavov v. Russia, 4 December 2015, § 229.

[20] European Court of Human Rights, Vukota-Bojic v. Switzerland, 18 October 2016, § 67; see also Leander v. Sweden, 26 March 1987, § 51; Uzun v. Germany, 2 December 2010, §§ 61-63; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, 28 June 2007, § 75; and Shimovolos v. Russia, 21 June 2011, § 68.

granted to the executive or to a judge to be expressed in terms of an 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 to give the individual adequate protection against arbitrary interference[21]. Accordingly, the Court has developed a number of 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;
- a 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.**[22]

In addition, as mentioned above, laws permitting the secret surveillance of communication must indicate the **conditions and circumstances** in which public authorities may resort to such measures. In a criminal context, these measures must be **suspicion-based**, i.e. they require the existence of a "reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures".[23]

b. Applicability of these principles beyond secret surveillance of communication to all covert interferences with private life

These principles have been developed by the Court mainly with regard to the secret surveillance of telephone or other communication, which is a particular serious interference with the rights of the citizen.

The underlying considerations and arguments are, however, in principle equally valid in the case

[21] See European Court of Human Rights, Roman Zakharov v. Russia, 4 December 2015, § 230, Malone v. United Kingdom, 2 August 1984, § 68; Leander v Sweden, 26 March 1987, § 51; Weber and Saravia v. Germany (dec.), 29 June 2006, § 94.

[22] See European Court of Human Rights, Roman Zakharov v. Russia, 4 December 2015, § 231; Amann v. Switzerland [GC], 16 February 2000, §§ 56-58; Valenzuela Contreras v. Spain, 30 July 1998, § 46; Prado Bugallo v. Spain, § 30, 18 February 2003; Weber and Saravia v. Germany (dec.), 29 June 2006, § 95; and Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, 28 June 2007, § 76.

[23] European Court of Human Rights, Roman Zakharov v. Russia, 4 December 2015, § 260; Iordachi v. Moldova, 10 February 2009, § 51. In Szabo and Vissy v. Hungary, 12 January 2016, § 71, the Court used the term "individual suspicion".

of other secret interferences with private life. In such cases citizens do not know about the interferences with their privacy. They do not have any influence on the decision-making process of the authorities, or to put forward their point of view on the matter. They do not have the possibility to clarify misunderstandings, to ask for the correction of errors, to ask for reconsideration of the matter, or to complain about unreasonable or arbitrary behaviour of state officials.

In cases involving open interferences with privacy, e.g. during a house search, both the affected citizens themselves and other persons like witnesses are able to verify whether the authorities act, in each particular case, within the limits of the law. They may monitor what is happening and communicate with the officers involved, they may immediately complain about unlawful or improper behaviour and take legal action if necessary. In contrast, if interferences are conducted in secret, all these possibilities do not exist. The whole process of deciding about which steps to take, and all powers connected with this, lie in the hands of the state authorities. It is "a field where abuse is potentially … easy in individual cases and could have … harmful consequences for democratic society as a whole"[24]. Accordingly, secret intrusions to privacy are by nature of a much greater intensity than open state measures, and the safeguards mentioned above must apply not only to telephone tapping, but to all secret measures interfering with privacy.

This conclusion is confirmed by the findings in the case of the Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, where the Court identified a number of shortcomings regarding the supervision of secret surveillance measures which included many categories similar to the Georgian operative-investigative activities, without distinguishing between the various measures (see case study below). The conclusion is further confirmed by the Recommendation, which contains a number of uniform rules about various special investigative techniques, without distinguishing between surveillance of communication and other techniques.

c. Application of these principles in the Georgian context

Most measures laid down in Article 7 para. 2 of the Georgian Law on Operative-Investigative Activities, may be considered secret interferences with privacy in the meaning just described, namely:

[24] European Court of Human Rights, Roman Zakharov v. Russia, 4 December 2015, § 233.

a) interviewing a person, if carried out by an undercover police officer or a police informer;
b) conducting surveillance of a person, in particular long-term surveillance;
c) carrying out a test purchase (usually carried out by an undercover police officer or police informer);
d) carrying out a controlled delivery (as soon as suspects or other affected persons are involved);
e) examining objects and documents, if conducted covertly and if relating to a person;
f) identifying a person, if carried out by an undercover officer or an informer;
g) censoring the correspondence of an arrested, detained and convicted person (if the censorship is not disclosed to the affected person);
h) obtaining electronic communication identification data;
j) infiltrating a secret collaborator or an operative into a criminal group in a prescribed manner;
k) setting up an undercover organisation in a prescribed manner (as soon as this organization gets in touch with particular persons);
l) monitoring Internet communications by observing and participating in open and closed Internet communications in the global information network (Internet), and creating situations of the illegal obtaining of computer data in order to identify a perpetrator.

The compatibility of these operative-investigative activities with human rights would require, inter alia, that the law

- describes the nature of the criminal offences which may give rise to an operative-investigative activity;
- contains a definition of the categories of people which may be affected by such measures,
- and provides for a limit on the duration of operative-investigative activities.

The law should also indicate that operative-investigative activities may only be initiated based on a sufficient factual basis, i.e. normally a reasonable suspicion that a criminal offence has been committed, or will be committed.

In addition, human rights require that a number of procedural safeguards are in place as regards the conduct, control and supervision of covert intrusions into privacy. These safeguards are discussed separately in Part 3 of this paper, below.

(1) The nature of the criminal offences

The text of the Law on Operative-Investigative Activities describes in Article 3 the objectives of operative-investigative activities, such as to "identify, put an end to and prevent a crime or any other unlawful act", to "identify a person who prepares, commits or who has committed a crime or other unlawful act", or to "obtain the necessary facts in a criminal case". Accordingly, operative-investigative activities may relate to any criminal offence and in addition, indeed, to any non-criminal unlawful act. In other words, any minor infraction of any law may give rise to covert intrusions of a citizen's privacy, even if the act does not constitute a criminal offence.

This situation raises strong concerns with regard to proportionality, since covert measures are very intensive interferences with citizens' rights. The Recommendation on special investigation techniques states – very adequately – that they should only be used where there is sufficient reason to believe that a "serious crime" has been committed or prepared, or is being prepared.[25] The Georgian law does not only apply to serious crimes; in fact not even any crime is necessary, just an "unlawful act".

In addition to proportionality concerns, the very wide scope of the law creates a risk of arbitrariness. It is evident that the police and other authorities do not have – and probably should not have – the capacity to use covert operative-investigative activities in order to prevent each and any breach of any law. They will have to select cases and set their priorities. However, these priorities are not laid down in the law. It is the executive which may decide from case to case as to whether they want to use covert methods or not. In many cases of minor infractions they will decide not to use covert methods, but in some cases they might decide to use them. There is a risk that such decisions on operative-investigative activities – targeting a citizen in the context of minor infractions or petty crime – will be made in an arbitrary manner.

(2) The categories of people which may be affected

The Law on Operative-Investigative Activities does not describe which persons may be affected by covert measures. It is not clear from the law which connection between a person and a breach of the law is necessary so that the person can be subjected to operative-investigative activities. According to the Law, operative-investigative activities may be used against suspects as well as

[25] Council of Europe, Committee of Minsters, CM/Rec(2017)6, Appendix, § 7.

their supporters, their family members, their friends, their neighbours, and perhaps also against people using the same city bus. Indeed, such measures can be used against each and every citizen, as long as they pursue the objectives mentioned in Article 3 of the Law. In a case against Hungary, the Court criticized that the legislation – which was restricted to preventing terrorist crimes – might be understood as "paving the way for the unlimited surveillance of a large number of citizens … 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 (…) and the prevention of any terrorist threat."[26] In a case concerning Moldova, even the expression "people involved in a criminal offence" was not considered adequate by the Court for describing the category of affected persons in a sufficiently clear manner.[27]

It follows that the Law on Operative-Investigate Activities does not describe, and limit, the categories of persons which may be subject to covert interferences with their right to respect for private life.

(3) Duration

It is an imperative requirement of proportionality that covert investigation activities are not longer applied than necessary. This means, inter alia, that the maximum duration of such measures are laid down in the law.

Article 8 of the Georgian Law on Operative-Investigative Activities regulates time limits in various contexts, in particular as regards criminal investigations. If an operative-investigative activity is related to the (suspected) criminal act of a person, it is normally limited to a period of seven days, with various possibilities of extension (Article 8 para. 1 b and e of the Law). However, these cases relate to cases involving "an instruction of the prosecutor, or of the investigator (…)" (b) and to an "inquiry and request of a body conducting operative-investigative activities" (e). They do not seem to cover the situation that a competent authority, of its own motion, starts a measure of operative work. In these cases there is no legal time limit for the operative-investigative activity.

This legal situation is not compatible with the European Convention on Human Rights.

[26] European Court of Human Rights, Szabo and Vissy v. Hungary, 12 January 2016, § 67.

[27] European Court of Human Rights, Iordachi v. Moldova, 10 February 2009, § 44.

(4) The factual basis for a decision to use covert measures

The Law on Operative-Investigative Activities does not require that there must be a reasonable suspicion that the person concerned has committed, or will commit a criminal act or other breach of the law. It is unregulated and unclear on which factual basis the competent authorities will take a decision to use covert measures. The requirement of a "reasonable suspicion", as laid down in the case-law of the European Court of Human Rights[28], is an important safeguard that citizens are not arbitrarily subjected to covert intrusions into their privacy.

The Recommendation provides in § 7, in a slightly more flexible manner, that "Special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared". The condition "sufficient reason to believe" is likely to be broader than "reasonable suspicion"; still it requires a factual basis upon which the authorities may act. Without such a basis – facts which allow the assumption that a crime has been committed or will be committed – it is not clear how the authorities will decide on the target persons in a rational, non-arbitrary manner.

Such a safeguard is missing in the Georgian legislation. The Law on Operative-Investigative Activities does not contain the requirement that such activities must be based on a reasonable suspicion or another sufficient factual basis indicating that a crime has been, or will be committed.

2. "Necessary in a democratic society"

As mentioned above, it is a requirement of human rights law that any interference with the right to respect for private life is "necessary in a democratic society" for pursuing one of the legitimate aims laid down in Article 8 para. 2 of the Convention.

In this respect, the Recommendation on Special Investigative Techniques provides that:

> 8. Member States should ensure proportionality between the special investigation techniques used and the legitimate aims pursued. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence and the intrusive nature of the specific special investigation technique used, should be made. Also the urgency and general complexity of the case could be considered.

[28] European Court of Human Rights, Roman Zakharov v. Russia, 4 December 2015, § 260; Iordachi v. Moldova, 10 February 2009, § 51.

> 9. Member States should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable the offence to be prevented, detected, investigated, prosecuted and supressed with adequate effectiveness.[29]

The requirement that any interference with the right to respect for private life must be "necessary in a democratic society" is reflected in Article 2 of the Law on Operative-Investigative Activities. According to this provision, activities under this law must constitute an appropriate and proportionate means for achieving a legitimate purpose. Consequently, if this provision is respected, all activities carried out when applying this law will respect the principles of necessity and proportionality. For clarification, a provision should be added to the Law that operative-investigative activities are a measure of last resort, i.e. they should only be used when their objective cannot be achieved by open law enforcement activity.[30]

Article 2, however, cannot correct the flaws which make the Law as such disproportionate. According to the Recommendation, the use of special investigative techniques must relate to a "serious" crime. The Member States of the Council of Europe have a certain discretion how they define a crime as being "serious", but this discretion is limited. It follows that for the prevention, detection or investigation of crimes that cannot be reasonably described as "serious", the use of special investigative techniques is considered by the governments as inappropriate and disproportionate. This must all the more be true if the operative-investigative activities are not even relating to a crime, but to "another unlawful act". If a certain act, while violating legal rules, is not considered criminal by the legislature, then such a (possible) minor breach of the law cannot justify the covert intrusion in the private lives of citizens.

As indicated above, a decision to use operative-investigative activities must be based on a sufficient factual basis. This is (also) a requirement of proportionality. Under the Rule of Law, the government cannot have the right to interfere with the private lives of each and every citizen without any factual indication that any unlawful activity has happened or will happen. Such an approach would not only lead, as indicated above, in all likelihood to arbitrary decisions about which persons will be the target of operative-investigative activities, but it is also grossly disproportionate.

Part 3. Control and supervision of operative-investigative activities

[29] Committee of Ministers, Recommendation CM/Rec(2017)6, Appendix.

[30] This is emphasised by the Committee of Ministers in its Recommendation: CM/Rec(2017)6, Appendix, § 9.

I. International standards and good practices as regards the supervision and control of covert activities

As regards control and supervision of special investigative techniques, the Committee of Ministers' Recommendation provides as follows:

> "4. (…) Domestic legislation should afford **adequate and effective guarantees against arbitrary and abusive practices** (…).
>
> 5. Member States should take appropriate legislative measures to ensure **adequate periodical review** of the implementation of special investigation techniques by judicial authorities or other competent authorities through **prior authorisation**, **supervision during the investigation** or **ex post facto review**.
>
> 6. Member States should ensure that an individual or legal person who claims to be the victim of a breach of his rights occasioned by the misuse of special investigation techniques shall have the **right of access to an effective remedy** before a competent authority."[31]

According to the case-law of the European Court of Human Rights, special safeguards are required in order to prevent unlawful or arbitrary executive action when measures affecting privacy are ordered and implemented without the knowledge of the affected person. The Court has summarized the applicable principles in the case of Roman Zakharov v. Russia:

> "232. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court (…) must be satisfied that there are adequate and effective guarantees against abuse. (…) 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" (…)..
>
> 233. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review

[31] Council of Europe, Committee of Ministers, CM/Rec(2017)6 of 5 July 2017, Appendix.

> should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. 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, judicial control offering the best guarantees of independence, impartiality and a proper procedure (…).
>
> 234. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his knowledge and thus able to challenge their legality retrospectively (…)."[32]

It follows from these considerations, and from similar reasoning already adopted in earlier cases[33] that independent review and supervision of secret surveillance measures should in principle be carried out

- before the beginning of the measure, securing that the legal requirements for adopting the measure have been met,
- during implementation of the measure, securing that it is carried out in accordance with the law,
- and after conclusion of the measure, to make sure that the whole measure has been lawful from the beginning to the end.
- In addition, normally the government must inform citizens that a covert measure was used against them, if and as soon as this disclosure can be made without jeopardizing the investigation or other important public interests, so that they may challenge the legality of the measure in Court.

[32] European Court of Human Rights, Roman Zakharov v. Russia, 4 December 2015, §§ 233, 234. See also Klass v. Germany, 6 September 1978, §§ 55, 56.

[33] See for example the case of Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, discussed below (case study Bulgaria).

The intensity of the review and supervision may depend of the intensity of the intrusion into privacy of a certain method in a given case. However, in the case of the Association for European Integration v. Bulgaria (see case study below), where the surveillance measures were very similar to operative-investigative activities under Georgian law, the Court did not distinguish between the various measures when describing the requirements of independent review and supervision.

II. Application of these principles in Georgia

The relevant provision of the Law on Operative-Investigative Activities is Article 21, which provides that:

> "1. Supervision of the strict and consistent observance of the law during operative-investigative activities, and of the lawfulness of the decisions made during the conduct of operative-investigative activities, shall be exercised by the Chief Prosecutor of Georgia and prosecutors subordinated to him/her."

1. No authorization by a court or other independent body

There is no rule in the Law on Operative-Investigative Activities which provides that such activities must be authorized, as a rule, by a court or other independent authority. Accordingly, in this respect the requirements of the Convention, as described above, are not fulfilled.

2. Prosecutorial supervision during implementation of the covert measure

According to Article 21 of the Law, as cited above, prosecutors are responsible for monitoring the legality of operative-investigative activities during their implementation. This provision is in line with human rights requirements, although the Law does not describe in detail the manner in which prosecutorial supervision is exercised.

3. The possibility to challenge operative-investigative activities in court

Article 6 of the Law on Operative-Investigative Activities provides that:

> "2. A person who considers that an operative-investigative measure conducted with respect to him/her has resulted in an unlawful restriction of his/her rights and freedoms may appeal against the lawfulness of such an operative-investigative measure to a higher state authority, prosecutor or court."

While this rule, as such, corresponds to the requirement that a remedy must be provided to the affected citizen, there is no provision in the Law to the effect that the citizen must be notified by state authorities once the operative-investigative activity has been concluded. In contrast, Article 5 of the Law provides that "Operative-investigative activities are highly classified". Exceptions to the absolute confidentiality of information obtained through such activities are foreseen for certain state organs, but not for the affected person.

Accordingly, the affected citizens will hardly ever know that an operative-investigative activity has been used against them. As a consequence, it is nearly impossible for them to challenge this measure in court. This legal situation is not compatible with the requirements of the Convention, as described above.

Part 4. Assistance provided by citizens to agencies conducting operative-investigative activities

I. The rights of the affected citizen

1. Police informants and private life

As shown in the previous sections, the use of an informant in order to receive information from citizens is an interference with their private lives which require a justification under Article 8 para. 2 of the Convention. For the reasons set out above, the rules of the Law on Operative-Investigative Activities do not fulfil the requirements developed by the European Court on Human Rights, since they do not indicate the nature of the criminal offences to which they are applicable, they do not describe the persons against which covert measures may be used, and they do not regulate the factual basis upon which such a measure may be ordered. Accordingly, like the other operative-investigative activities described in the Law, the use of police informants, under the present law, is not compatible with the Convention.

2. Police informants and fair trial

In addition to privacy concerns, the involvement of undercover police officers or informants may also raise an issue under the fair trial principle (Article 6 of the Convention) in the so-called entrapment cases. While the Court regularly accepts the use of undercover agents as a legitimate investigative technique for combating serious crimes, this technique requires that clear, adequate and sufficient procedural safeguards set permissible police conduct aside from entrapment. The public interest cannot, in the Court's view, justify the use of evidence obtained as a result of police entrapment, in particular in cases where police have incited a person to commit on offence which would not have been committed otherwise.[34] It is a legitimate purpose of police and other government authorities to prevent and prosecute, but not to instigate crime. In cases of entrapment, the trial is unfair from the outset.[35]

When the relevant facts can be established in a particular case, the Court conducts a "substantive test" in order to ascertain whether it was a case of entrapment. There may be other cases, however, where the facts are less clear, where the defendant claims that the offence has been incited by the police, but this claim is disputed by the prosecution. In such cases the Court conducts a "procedural test", requiring that the trial court examines the claim of entrapment. In the recent case of Tchokhonelidze v. Georgia, the Court described these tests as follows:

> "44. (…) Under the substantive test, when examining an applicant's arguable plea of entrapment, the Court will enquire, as a first step, into whether the authorities had good reasons for mounting a covert operation. In particular, they must show that they were in possession of concrete, objective and verifiable evidence showing that initial steps have been taken to commit the acts constituting the offence, and that the criminal act was already underway at the time when the police intervened (…). This principle rules out, in particular, any conduct that may be interpreted as inciting the applicant to commit an offence that would otherwise not have been committed, such as taking the initiative in contacting the applicant, repeating an offer despite having received an initial refusal, insistent prompting, the promise of financial gain, or appealing to the applicant's sense of compassion (…)
>
> 45. Where the authorities claim that they acted upon information received from a private individual, the Court draws a distinction between an individual complaint and information coming from a police collaborator or informant (…). A collaborator or informant would

[34] See European Court of Human Rights, Teixeira de Castro v. Portugal, 9 June 1998, § 36, and Nosko and Nefedov v. Russia, § 50, 30 October 2014, Tchokhonelidze v. Georgia, 28 June 2018, § 44.

[35] European Court of Human Rights, Teixeira de Castro v. Portugal, 9 June 1998, § 39.

> run a significant risk of extending their role to that of agents provocateurs, in possible breach of Article 6 § 1 of the Convention, if they were to take part in a police-supervised operation. It is therefore crucial in each case to establish if the criminal act was already under way at the time when the source began collaboration with the police (…) The Court has found that the line between legitimate infiltration by an undercover agent and the instigation of a crime is more likely to be crossed if no clear and foreseeable procedure was set up under the domestic law for authorising and implementing undercover operations – all the more so if they were also not properly supervised. It has considered judicial supervision as the most appropriate means in cases involving covert operations (…). A lack of procedural safeguards in the ordering of an undercover operation generates a risk of arbitrariness and police entrapment (…).[36]
>
> 46. In cases where the lack of file disclosure or the controversy of the parties' interpretation of events precludes the Court from establishing with a sufficient degree of certainty whether the applicant was subjected to police incitement, the procedural aspect becomes decisive. (…) Although the Court will generally leave it to the domestic authorities to decide what procedure must be followed by the judiciary when faced with a plea of incitement, it requires such a procedure to be adversarial, thorough, comprehensive and conclusive on the issue of entrapment, with the burden of proof on the relevant prosecution authority to demonstrate that there was no incitement. (…) The domestic courts' duty to ensure the overall fairness of the trial requires, inter alia, that the undercover agents and other witnesses who could testify on the issue of incitement should be heard in court and be cross-examined by the defence, or at least that detailed reasons should be given for a failure to do so (…)."

Test purchases of drugs with participation of an informant are typical cases where the risk of entrapment exists. In a number of such cases the Court found a violation of Article 6.[37]

The legal situation in Georgia as regards test purchases and other situations where there is a risk of entrapment raises a number of concerns.

1. The Court requires that "the authorities had good reasons for mounting a covert

[36] European Court of Human Rights, Tchokhonelidze v. Georgia, 28 June 2018, §§ 44, 45; referring to Ramanauskas v. Lithuania [GC], 5 February 2008, § 67; Malininas v. Lithuania § 37, 1 July 2008; and Vanyan v. Russia,, §§ 11 and 49, 15 December 2005; Khudobin v. Russia, 26 October 2006, § 135; Furcht v. Germany, 23 October 2014, § 53; Bannikova v. Russia, 4 November 2010, §§ 49, 50.

[37] European Court of Human Rights, Teixeira de Castro v. Portugal, 9 June 1998; Vanyan v. Russia, 15 December 2005; Veselov v. Russia, 2 October 2012, and others. Other cases concern bribery (Ramanauskas v. Lithuania, 5 February 2008, Tchokhonelidze v. Georgia, 28 June 2018).

operation", in that they had "concrete, objective and verifiable evidence" showing that the defendant had already taken steps to commit the criminal act. Such a requirement is not mentioned in the Georgian Law on Operative-Investigative Activities; according to the letter of the law, test purchases may be carried out in situations where there is no suspicion of past or present illegal activity. In the interest of legislative clarity, and in order to avoid unlawful entrapment, it is desirable that a requirement of reasonable suspicion is included in the law, for example in the principles of operative-investigative activities (Article 2) or in the legal guarantees for protection human rights and freedoms (Article 6 of the Law).

2. The Court considers that "the line between legitimate infiltration by an undercover agent and the instigation of a crime is more likely to be crossed if no clear and foreseeable procedure was set up under the domestic law for authorising and implementing undercover operations – all the more so if they were also not properly supervised." A comparative study carried out by the Court on the situation in 22 Council of Europe member states showed that almost all countries provide for a special procedure as regards the possibility of the police to carry out undercover operations, in particular in drug-trafficking cases. In most countries there is exclusive or shared responsibility of the judicial bodies in the authorisation procedure, although in some the decision lies with the public prosecutor, the administrative authorities or high-level police officials.[38]

   The Law on Operative-Investigative Activities does not require that infiltration by an undercover agent be ordered by a court or other authority independent from the authority carrying out the operation, which was criticized by the Court in the Tchokhonelidze case[39]. In fact, the authorization procedure is not regulated by the Law.

3. Under the Law on Operative-Investigative Activities, the decision to use an undercover agent or informant is not subject to judicial supervision. Accordingly, there is a lack of procedural safeguards which, in the words of the Court, "generates a risk of arbitrariness and police entrapment".

II. The rights and status of the informant

[38] European Court of Human Rights, Veselov v. Russia, 2 October 2012, §§ 50-52.

[39] European Court of Human Rights, Tchokhonelidze v. Georgia, 28 June 2018, §§ 51, 53.

1. The positive obligation to protect life and integrity of the informant

International human rights standards require that the government takes positive steps to protect the lives of their citizens. Since the activities of a police informants may carry specific dangers for life or physical integrity, the government has a special responsibility with regards to the rights of informants.[40]

The Law on Operative-Investigative Activities regulates in Article 17 the "Legal and social protection guarantees for citizens assisting agencies conducting operative-investigative activities". In line with paragraphs 1, 2 and 7 of this Article, informants shall be protected by the state, and in the case of a real threat to life, health or property of an informant the state shall take appropriate protection measures, including special security measures if necessary.

It appears that Georgian legislation is in line with international human rights standards as regards the protection of informants.

2. Legal policy considerations as regards the use of police informants

The use of informants is useful and necessary in cases where terrorist activities, organised crime of other serious crimes are investigated, or if serious dangers for the community are to be prevented.

Nevertheless, the use of informants may be problematic in many cases. Regardless of whether their use is lawful in a particular case or not, legal policy considerations may suggest that informants should not be used as a routine measure, but with appropriate care and restraint. This issue has been discussed extensively in the United States of America.[41] In the context of this paper, the practical problems connected with the use of informants can only briefly be pointed out:

a. Informants are typically recruited from criminals who want to avoid a harsh sentence. In exchange for the promise to provide information, charges are dropped or a sentence reduced. If they go free, they will typically continue to be involved in certain criminal activities, for example drug-dealing.

---

[40] In the case of D.F. v. Latvia, 29 October 2013, the European Court of Human Rights found a violation of Article 3 of the Convention because the government had failed to secure a former informant's safety in prison.

[41] See, for example, A. Natapoff, Secret Justice: Criminal Informants and America's Underground Legal System. Prison Legal News, June 2010, p. 1.

b. Since law enforcement have an interest in continuing the cooperation with informants, they may be protected by police even if they commit new crimes.

c. The victims of informants' criminal activity are ignored.

d. If the criminal justice system routinely uses a great number of informants, the message to the public is that "crime is negotiable and justice is for sale".[42] In some cities and neighbourhoods in America, "Stop snitching" campaigns have been initiated.

e. Information received by informants is often unreliable. They are expected to provide evidence for securing convictions, and they have a self-interest to comply with the request made by the police. So they may feel tempted to provide damning evidence even if it is not true.

f. Informants are sometimes used to circumvent the usual safeguards applicable in criminal investigations. For example, an informant is sent to a suspect to ask him questions about his criminal activities, without securing that he may make use of his right to remain silent.

g. The "deals" between informants and police are concluded and implemented in the shadow. In view of the important issues involved and the dangers to which the informant may be subjected, they should be regulated by the law, which they often are not.

h. Using a high number of informants is a very problematic social policy. Informants may destroy social connections and social cohesion. In fact, informants are typically used in neighbourhoods where poor people or persons belonging to minorities are living.

The many problems connected with the use of informants have led the legislations of some states to limit and restrict the use of police informants.

Conclusion

Operative-investigative activities under Georgian law, which are normally of a covert nature, typically interfere with the right of respect to private life of citizens. According to international human rights standards, covert measures constitute very intense interferences with human rights. They may be used only exceptionally in order to protect society from serious crimes. The law must describe clearly which crimes may give rise to covert measures and define the persons who may be the target of such activities. In addition, covert measures may only be initiated on a

[42] A. Natapoff, Secret justice, section V.

sufficient factual basis for assuming that a serious crime has been, or will be, committed or prepared, and they must be limited in duration. Finally, a number of procedural safeguards must be in place: covert measures must be authorized by an independent body, must be monitored during their implementation, and, as a rule, the affected citizens must be informed subsequently so that they may take legal action.

According to the analysis conducted in this paper, the compatibility of Georgian law with these requirements is in serious doubt. These concerns relate in particular to the following points:

1. Operative-investigative activities may be used under Georgian law not only in the fight against serious criminal offences, but with regard to any criminal offence and, indeed, against any unlawful act even if it is of a non-criminal nature.

2. The categories of persons who may be subjected to operative-investigative activities are not defined in the law, so that all citizens may be affected by such a measure, even if they are not or only very remotely connected to any illegal activity.

3. The duration of operative-investigative activities is not limited in all cases.

4. Georgian law does not require that a sufficient factual basis is necessary for initiating operative-investigative activities.

5. No judicial or other independent authorisation is necessary for initiating operative-investigative activities under Georgian law.

6. Georgian law does not provide that citizens are informed once an operative-investigative activity has been concluded. As a result, it is virtually impossible to challenge operative-investigative activities in court.

In addition, our analysis raises a number of concerns, in the light of the right to a fair trial, as regards test purchases and other situations where there is a risk of entrapment. According to the case-law of the European Court of Human Rights, test purchases may only take place on a sufficient factual basis that the affected person has already the intention to commit a crime, and they should at best be ordered by a judge or other independent authority. As pointed out above, Georgian law does not correspond to these requirements, so that there is a risk that operative-investigative activities lead to unlawful entrapment. In such a case, it is likely that the results of operative-investigative activities cannot be used for obtaining a conviction of the affected person in subsequent criminal proceedings.

In sum, it seems that the Georgian Law on Operative-Investigative Activities does not adequately take into account that covert intrusions into citizens' privacy constitute very serious and intense interferences with their human rights which should only be used in exceptional cases, and accompanied by legal safeguards ensuring that these powers will not be used in an arbitrary or

disproportionate manner. In the light of international human rights standards, a major reform of this Law appears necessary.

Annex 1. Case Study Bulgaria

The case of
The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria

1. The case before the European Court of Human Rights

On 28 June 2007 the European Court of Human Rights issued the judgment in the case of the Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria.

The applicants, a non-profit-association and a lawyer, complained that, under the Special Surveillance Means Act (SSMA) of 1997, they could be subjected to surveillance measures at any time without notification.

Special means of surveillance include, according to Articles 5-11 SSMA: observation (visual and by technical devices), tapping, surveillance, penetration of premises or objects, marking, interception of mail, controlled delivery, trusted transaction, undercover officers, recording and photographing. This means may be used against "persons who are reported to, and for whom there are reasonable grounds to presume that they are preparing to commit, are committing, or have committed grave intentional crime ..." (Article 12) by institutions including "the National Police Directorate General, the Directorate General for Combating Organized Crime, the Border Police Directorate General, the Internal Security Directorate, the regional directorates of the Ministry of Interior, the specialized directorates" (Article 13).

The Court considered that while in certain respects Bulgarian law fully comports with the requirements of Article 8 of the Convention, in other respects it falls short. The SSMA circumscribed the purposes for which covert monitoring may be used: preventing or uncovering serious offences or protecting national security. Such monitoring could be used only if there are grounds to suspect that a serious offence is being planned or is or has been committed, and only if the establishment of the facts by other methods are deemed unlikely to succeed. Surveillance could only be allowed pursuant to a written application giving reasons, which may be made solely by the heads of certain services. The warrant authorising the surveillance could be issued only under the hand of the president or the vice-president of a regional court, a military regional court, or a court of appeals. This judicial authorisation had principle to be given before the surveillance has taken place. Surveillance could normally be authorised for a maximum of two months. It thus seemed that during the initial stage, when surveillance is being authorised, the SSMA provided substantial safeguards against arbitrary or indiscriminate surveillance.

However, the Court also examined whether such safeguards existed during the later stages, when the surveillance was actually carried out or had already ended.

It noted

- that the SSMA did not provide for any review of the implementation of secret surveillance measures by a body or official that was either external to the services deploying the means of surveillance or at least required to have certain qualifications ensuring its or his independence and adherence to the rule of law,

- that the SSMA made no provision for the judge to be informed of the results of the surveillance or require the judge to review whether the provisions of the law had been complied with,

- the lack of regulations specifying with an appropriate degree of precision the manner intelligence obtained through surveillance was screened, the procedures for preserving its integrity and confidentiality and the procedures for its destruction,

- that overall control over the system of secret surveillance was entrusted solely to the Minister of Internal Affairs – who was directly involved in the commissioning of special means of surveillance – and not to independent bodies, and that the manner in which the Minister was to exercise this control was not set out in the law.

- that the law did not provide for the notification of persons subjected to monitoring under any circumstances or at any time, even after it had ceased, and that the persons concerned were accordingly unable to seek redress for unlawful interferences with their Article 8 rights,

- and, finally, that the statistics showed that the system of secret surveillance in Bulgaria had been overused.

In sum, the Court considered that Bulgarian law did not provide sufficient guarantees against the risk of abuse inherent in any system of secret surveillance, and that the interference with the Article 8 rights of the applicants had therefore not been "in accordance with the law".

2. Supervision of the execution of this judgment by the Committee of Ministers

Since 2007, this case, together with some similar Bulgarian cases, is under the supervision of the Committee of Ministers; it has not yet been closes. Still, the Bulgarian authorities have taken a number of general measures in order to comply with the judgment, including:

- an independent National Bureau monitoring the secret surveillance system ("the Bureau") has been created. The Bureau presents annual reports to the Parliament and gives mandatory instructions to competent bodies. It informs of its own motion persons who have been subject to unlawful secret surveillance, if this can be done without harming certain countervailing interests.

- as regards judicial authorisation and control over the use of secret surveillance in criminal matters, secret surveillance can now be used only for investigating or preventing an exhaustive list of serious criminal offences,

- specific time limits (ranging from 20 days to six months) have been introduced for the use of surveillance depending on its purpose,

- the National Bureau noted that the reasoning of judicial authorisations and refusals (including partial refusals) has considerably improved since 2015. The judge also receives a copy of the evidence obtained and a report after the end of the surveillance.

- as regards the use of secret surveillance in relation to terrorist offences, since December 2016, the requirements applicable in respect of such requests are less strict and authorisation may be granted even if there is no identification data available as to the persons or objects under surveillance. The initial authorisation can be valid up to two years (without periodic judicial review) and can be extended to three years by a judge.

As a consequence of these developments and achievements, the Committee of Ministers took a decision stating, inter alia, the following:

"The Deputies

(…)

3. recalled the important progress made in the areas of judicial review of secret surveillance requests, including in the context of protection of national security, of the external control over the use of secret surveillance, the introduction of a domestic compensatory remedy for unlawful secret surveillance, as well as the decrease in the use of secret surveillance;

4. encouraged the authorities to introduce clear rules as to whether secret surveillance can be used to protect national security, if a person is not suspected of preparing or committing a criminal offence; encouraged them also to ensure that the Specialised Criminal Court has at its disposal adequate means for examining the high number of surveillance requests it receives and to set up a common database for surveillance requests or to adopt other measures to minimise the risk of duplication of requests;

5. invited them to adopt legislative measures to reinforce the guarantees for the qualification and for the independence of the members of the National Bureau monitoring the secret surveillance system from the institutions it oversees and to ensure that it has access to all the material necessary for it to carry out its tasks, including material on which surveillance requests are based, as required by the European Court's case-law;

6. invited them also to provide information on the precise investigative powers of the courts examining claims for unlawful secret surveillance where the claimant has not been formally notified of the surveillance by the Bureau or in criminal proceedings and, if necessary, to reinforce these powers through legislative measures; invited them to indicate whether a person affected by unlawful secret surveillance can request the destruction of the intelligence gathered, taking into account also the countervailing interests;

7. as concerns surveillance authorisations in national security or terrorist contexts, which can currently be valid for up to two years, encouraged the authorities to introduce a requirement for periodic judicial review at shorter intervals; invited them also to provide information on the other outstanding questions, namely on the competence of the Bureau to notify legal persons of illegal surveillance, on the rules governing the screening, preserving the confidentiality and integrity and destruction of the intelligence and on whether the Special Surveillance Means Act restricts the use of intelligence falling outside the scope of an initial authorisation to situations in which it concerns other serious criminal offences." [43]

3. Significance in the Georgian context

The case is significant for Georgia since the Bulgarian "special means of surveillance" are similar to the operative-investigative activities conducted by the Georgian authorities. It should be noted that, unlike the Georgian law, even before 2007 the application of the Bulgarian law was limited to "serious offences", and the law required that there were "reasonable grounds to presume", i.e. a sufficient factual basis, that the persons concerned were involved in such an offence. Still the Court identified a number of shortcomings as regards the independent review of the secret surveillance measures, the judicial supervision and other safeguards, as described above.

It may also be of interest in the Georgian context that Bulgaria has set up, as a reaction to this judgment, an independent National Bureau monitoring the secret surveillance system.

The combination of the requirement of a judicial authorisation – which must normally be issued ex ante – with the monitoring conducted by the National Bureau may be considered a good practice in safeguarding the rights of persons subjected to a secret surveillance measure.

[43] Committee of Ministers, 4-6 June 2019, CM/Del/Dec(1019)1348/H46-5.

Annex 2. Case Study Germany

Judgment of the Federal Constitutional Court of 20 April 2016 on the Law on the Federal Criminal Office (Bundeskriminalamtgesetz – BKAG)

Case no. 1 BvR 966/09, 1 BvR 1140/09,
available at www.bverfg.de (in German and English language)

The applicants complained that certain powers of the Federal Criminal Office (Bundeskriminalamt – BKA) to conduct measures of covert surveillance violated their fundamental rights under the German Constitution.

1. The powers of the Federal Criminal Office

In order to protect citizens and the state against threats from international terrorism, the BKA had the powers, under the BKAG as amended 2009, to conduct certain covert surveillance measures. They included, inter alia,

- the observation of persons,

- the application of tracking devices and other technical means for observation,

- the taking and recording of photographs and videos,

- the use of police informers and undercover investigators,

- the collection of telecommunication traffic data

as well as many other measures seriously interfering with privacy, such as the covert monitoring and recording of non-public conversations, the visual and acoustic surveillance of private homes and the monitoring of telecommunications. The BKA was also empowered to share the data obtained by way of such measures, under certain conditions, with other authorities in Germany and abroad.

2. The constitutional standards

In its judgment of 20 April 2016, the Constitutional Court considered that many of the covert surveillance measures under the BKAD constitute serious interferences with privacy. Such interferences may be justified in the context of prosecuting or preventing serious crimes, in particular crimes against the life or liberty of persons. In such cases, proportionality requires that a number of safeguards are in place:

a. Covert surveillance measures may be used only for **protecting particularly weighty rights and legal interests.** These include, according to the Court, life, limb and liberty of the person as well as the existence and the security of the State, but not, for example, all aspects of property rights.

b. Such measures are generally only proportionate if there are **strong factual indications** that **a sufficiently specific foreseeable threat** to these legal rights or interests exists. General experience alone cannot justify an interference.

c. Persons may only be the **target** of covert surveillance measures if, based on objective evidence, they may reasonably be considered to be **involved** therein. A mere possibility based primarily on the **intuition** of the security authorities that further intelligence might be obtained is **not sufficient**.

d. Human dignity requires that the state respects, with regard to each person, a **core area of private life** which includes, for example, the possibility to express feelings or opinions of a highly personal nature, to enter into confidential communication on such matters, as well as forms of sexual expression. Communication about criminal acts does not fall into this area.

The core area of private life is beyond the state's reach; even paramount public interests cannot justify an interference with this area. The law must provide **safeguards** ensuring that even unintentional interferences with this area are ruled out as far as possible, and that data which are nevertheless obtained by way of an intrusion into the core area of private life will be deleted immediately and will not be used for any purpose.

e. Covert measures seriously interfering with privacy require, as a rule, **prior review by an independent body**, for example a court, on the basis of a well-substantiated application made by the competent authority. The application must provide comprehensive information on the situation in question.

f. The affected persons must be able to **challenge effectively** the legality of covert surveillance measures in court. In particular, in order to enable them to do this, legislation must provide that **persons are generally notified subsequently of the surveillance measures** taken against them. Exceptions are possible, but only as far as they are absolutely necessary and confirmed by a judge.

g. Serious violations of the legal conditions for interferences with privacy must lead to consequences such as **compensation**.

h. Since individual legal protection against covert surveillance measures can be ensured only to a very limited exent, such measures must be subject to **effective supervisory control**, carried out for example by **independent data protection commissioners**. The BKA must also **report**

regularly to Parliament on the exercise of the power to use covert surveillance measures, and thus subject the data collection to democratic oversight and review.

3. Compatibility of the BKAG with the constitutional standards

a. The Constitutional Court found that the powers laid down in the BKAG were applicable only to threats of terrorist crimes. Accordingly, they were designed to protect life and limb of citizens as well as the security of the state. These are **sufficiently weighty rights and interests** (see requirement 2a., above).

b. However, the Court found that most of the challenged provisions of the BKAG did not state clearly that **strong factual indications** substantiating a sufficiently specific foreseeable threat are necessary for carrying out the surveillance measure. Thus, the BKAG did not provide the authorities and courts with sufficiently defined criteria for assessing the legality of the measure in question, as required (see 2b, 2c above).

c. The Court considered also that the impugned provisions of the BKAG allowed measures which can in part typically result in the monitoring of such confidential situations from which the state is strictly excluded. Thus, in order to safeguard the **core area of private life** both with respect to data collection and to data analysis, the law had to include specific protective provisions. Such provisions, however, were lacking.

d. As to the **prior review carried out by an independent body**, the BKAG required a direct judicial order for the initial ordering of a measure only if undercover investigators are to be employed. As to other possible interferences, the initial order could be made by the Federal Criminal Office, and only an extension of such an order required judicial confirmation.

The Constitutional Court considered that an **initial judicial order is necessary in all cases of serious interferences with privacy, including the monitoring and recording of non-public speech and the use of police informants as well as long-term observation including the use of visual recordings or tracking devices**. Exceptions are only possible in cases of immediate danger.

e. The Court found also that the **provisions aiming to guarantee transparency, legal protection and judicial** review did not completely satisfy the constitutional requirements. They lacked adequate specifications on regular mandatory review, on a comprehensive documentation requirement which allows the full and effective review of the surveillance measures in question, and on reporting duties *vis-à-vis* Parliament and the public. Finally, the rules on the deletion of the collected data also only partially satisfy constitutional requirements.

f. The Court also found some other violations of the constitution, relating, for example, to the powers of the Federal Criminal Office to monitor ongoing telecommunication, to conduct acoustic surveillance of private homes, and to share data with other domestic or foreign authorities.

4. Reaction by the legislature

On 1 June 2017 the legislature adopted a new BKAG (Bundesgesetzblatt 2017 I, p. 1354) which complied with the constitutional requirements, as stated by the Federal Constitutional Court.

5. Significance for Georgia

The case is significant for Georgia in various respects.

a. It covers police powers to conduct covert surveillance measures like long-term observation, the use of undercover officers and police informers, as well as the collection of telecommunication traffic data. To a large extent, these are measures which would be considered operative-investigative activities under Georgian law.

b. The safeguards developed by the Constitutional Court are applicable in the context of prevention of future criminal acts, not only for the investigation of crimes already committed.

c. The judgment is founded, of course, on German constitutional law. The essential parts, however, are based on proportionality considerations which may be considered a general principle of human rights law, be it national or international.

d. The Court derives many specific requirements from the proportionality principle. These requirements appear to be rather strict even though they are applicable to very serious threats relating to terrorism.

e. The judgment confirms that covert surveillance measures should only be used for fighting serious crime, or for protecting otherwise important rights or legal interests, and that they may only be ordered on a strong factual basis indicating a specific threat.

f. The Constitutional Court considers long-term observation, the use of undercover officers and police informers, as well as the collection of telecommunication traffic data to be very serious interferences with privacy which, in principle, must always be subject to a prior review by an independent body, normally a court. As a rule, citizens must be notified subsequently of the surveillance measures taken against them.

g. According to the Court, human rights require that covert surveillance measures must be subject to effective supervisory control, carried out for example by independent data protection

commissioners, and that the police reports regularly to Parliament on the exercise of their power to use covert surveillance measures.

h. The idea of a "core area of private life" to which the state has no access is a specific requirement of German constitutional law, which is based on human dignity. This idea apparently goes beyond the requirements of international human rights law as it stands today. Courts of other countries may take this as an inspiration and consider whether the idea of an inaccessible core area of private life might or should be derived, by way of interpretation, from their constitution as well.

Indeed, Georgian Law already seems to have recognized the idea of such a core are of private life. According to Article 6 para. 4 of the Law on Operative-Investigative Activities,

> "Information that has been obtained by operative-investigative activities and that is not related to a person's criminal activities, but contains details of his/her private life, may not be disclosed or used for any purpose. Such information may not be stored and it must be immediately destroyed. The destruction of such information shall be notified to the Chief Prosecutor of Georgia and the court in the territory where the operative-investigative measure has been conducted or the court according to the place of investigation."

i. In general, the situation under German constitutional law may be considered a good practice as regards the legal regulation of covert surveillance measures in the context of crime prevention.