საერთაშორისო გამჭვირვალობა–საქართველო
TRANSPARENCY INTERNATIONAL GEORGIA

Assessment of the Georgian legislation on telephone interception in the light of the European Convention on Human Rights standards

Summary

The constitutional right to privacy – a right also guaranteed by Article 8 of the European Convention on Human Rights (ECHR), ratified by Georgia in 1999 – might run the risk of being violated since the Georgian domestic law governing telephone tapping does not contain sufficient guarantees against abuse by the national authorities. The legislative regime neither satisfies the requirement of foreseeability nor provides for sufficient safeguards against arbitrary interception and abuse as provided by the standards developed by the European Court of Human Rights (ECtHR):

- **Categories of crimes:** Currently under the Law on Operative Investigative Activity telephone interception (in urgent and non-urgent cases) can be requested for all crimes provided by the Criminal Code when there is a resolution of the prosecutor, in the vast majority of the crimes when there is a motion of the victim or alternatively for any crime punishable by criminal legislature with more than two years imprisonment. This is a far reaching provision, which is contrary to the human rights standards.
- **Categories of persons:** The Law on Operative Investigative Activity does not expressly make reference to the categories of persons that might be liable to interception. However, Article 2, which enumerates the aims of the special measure, gives the possibility to infer categories of persons that might be subjected to surveillance. Also, Article 3 (11) of the Code of Criminal Procedure provides for a reasonable suspicion test that read together with the mentioned law allows concluding that persons satisfying the reasonable suspicion test might fall under the category of persons that might be subjected to interception. However, when it comes to third persons *i.e.* those against whom there is no reasonable suspicion that they have committed a crime but might be somehow related to the case, the law is silent. To exclude abuse the specialized law should expressly provide for the categories of persons liable to have their telephones tapped.
- **Interception to be requested base on the existence of a reasonable suspicion:** The Law on Operative Investigative Activity does not expressly provide for the degree of reasonableness of the suspicion against a person who may be liable to interception. Article 3 (11) of the Code of Criminal Procedure provides for a reasonable suspicion test to be applied for conducting an investigatory action (including wiretapping). It is better if the

Law on Operative Investigation Activity expressly specifies that the test directly applies to wiretapping, like it does in other investigatory actions.

- **Duration:** The Law on Operative Investigative Activity is silent in regard to the initial period after which an interception warrant will expire. According to the Recommendation of the Supreme Court of Georgia from 4 January 2013, a court shall determine the duration of the phone interception for 1 month. This is in accordance with the human rights standards; however such a recommendation does not have an obligatory power. The law also does not provide for a concrete period of time for an extension and how many times it can be renewed. It is important that the law expressly provides for the limits of the duration of a surveillance measure in order to protect against arbitrary or excessive use of phone interceptions.
- **Interception should be a last resort measure:** The Law on Operative Investigation Activity is silent on this matter. This allows concluding that virtually phone interception could be used even in cases when other less intrusive methods are available.
- **The procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communication the data to other parties:** The Law on Operative Investigation Activity contains several provisions on the use of data obtained through wiretapping. The Criminal Code provides for criminal responsibility for illegal dissemination of personal data. Nevertheless, the law does not provide for any procedure concerning the transmission of data between different authorities, neither it includes precise regulations specifying the manner of screening the intelligence obtained through surveillance, or the procedures for preserving its integrity and confidentiality and the procedures for storing and destruction.
- **Circumstance under which the recordings or tapes may or must be erased or destroyed:** The Law on Operative Investigation Activity specifies that collected data, which does not relate to the criminal activities of the person, but includes compromising information, should not be stored and must be destroyed immediately. This is an important safeguard but has a limited application, since it does not oblige the competent body to delete any other type of personal information collected during interception which proved to be unrelated to the criminal activity. The law is completely silent on the destruction of collected data in general after for example proceedings are finalized or after the completion of a certain period of time.
- **Precautions have to be taken to protect privileged communication between attorney and client:** The Georgian legislation guarantees the attorney-client communications but it does not provide for any procedure which would give substance to the above mentioned guarantee. This is not in accordance with the ECtHR standards. There is a need for clear rules that would reflect which concrete steps are to be taken to ensure that this guarantee is respected in practice and does not remain only a theoretical guarantee.
- **Oversight mechanism:** The control and supervision of the secret surveillance conducted by the competent entities is realized by the chief of the operative-investigation

organization who is personally responsible, the legality of the activities is controlled by the minister of justice and the prosecutors under his or her control. With regard to the court control, the judge gives permit for telephone interception. However the detailed manner in which control by the chief of the operative-investigation or the minister of justice or the prosecutor is effectuated is not set out in the law. Additionally, since the ultimate control is realized by the executive power this could raise doubts regarding its independence and impartiality. The oversight mechanism should be entrusted to an independent authority.

General overview

The Georgian Constitution ensures the protection of the private life, place of personal activity, personal records, correspondence, and communication by telephone or other technical means (Article 20). These fundamental rights are not absolute and they can be restricted. However, the state has to justify all kind of restriction of these freedoms and is obliged to protect these freedoms. The constitution states that the restriction of these fundamental freedoms is allowed with the permission of the court or without such a decision in cases of the urgent necessity defined by law.

The telephone interception in Georgia is regulated by the Law on Operative Investigation Activity that allows law enforcement agencies to use *inter alia* wiretapping (Article 7).

According to the case-law of the ECtHR interception of mail, telephone and email communications including those made in the context of business dealings, are covered by the notions of "private life" and "correspondence" in Article 8 (1) of the European Convention of Human Rights. Theoretically any interception may be considered as an interference into the right to privacy of communications. Therefore an interference must be **"in accordance with the law"**. That means that first, the impugned measure must have some basis in domestic law. Second, the domestic law must be compatible with the rule of law and accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him (*Rotaru v. Romania*, para. 52; *Liberty and Others v. UK* para. 59; and *Iordachi and Others v. Moldova* para. 37).

The ECtHR has summarised in *Weber and Saravia v. Germany* its case-law on the requirement of legal "foreseeability" in the field of secret surveillance:

"93. ... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, inter alia, Leander v. Sweden, judgment of 26 August 1987, Series A no. 116, p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, inter alia, Malone, p. 32, § 67; Huvig, pp. 54-55, § 29; and Rotaru). ***It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated*** (see Kopp v. Switzerland, judgment of 25 March 1998, Reports 1998-II, pp. 542-43, § 72, and Valenzuela Contreras v. Spain, judgment of 30 July 1998, Reports 1998-V, pp. 1924-

25, § 46). The domestic law ***must be sufficiently clear*** in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see Malone, ibid.; Kopp p. 541, § 64; Huvig, pp. 54-55, § 29; and Valenzuela Contreras, ibid.).

94. Moreover, since the implementation in practice of measures of secret surveillance of communications 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 legal discretion 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 (see, among other authorities, Malone, pp. 32-33, § 68; Leander, cited above, p. 23, § 51; and Huvig, pp. 54-55, § 29)".

This means that the law on which the phone interception is based has to *set out clearly in which circumstances and subject to which conditions communications may be intercepted*. In addition, ECtHR has established criteria a law has to satisfy so as to be sufficiently precise and to provide safeguards against arbitrary use:

"95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in **statute law** in order to avoid abuses of power: ***the nature of the 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 the tapes destroyed*** (see, inter alia, Huvig, p. 56, § 34; Amann, cited above, § 76; Valenzuela Contreras, cited above, pp. 1924- 25, § 46; and Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003)."

In addition, the ECtHR has held that the legal basis for phone interceptions ***has to provide rules ensuring that information falling under the lawyer-client privilege is not intercepted*** (*Iordachi and Others v. Moldova*, *Kopp v. Switzerland*).

Categories of crimes

A. ECtHR standards

The law providing the legal basis for phone interceptions has to *specify the categories of crimes* which may give rise to a phone interception. This can be done in (at least) two forms:

- The relevant crimes are defined according to specific criteria

- A catalogue of specific crimes which may prompt a phone interception is included in the law

In *Kennedy v UK*, the ECtHR has scrutinized the monitoring of phone conversations by British authorities. The British legal framework foresees that phone interceptions may *inter alia* be authorized 'for the purpose of preventing or detecting serious crime'. Serious crime is defined as an offence for which a person who has reached the age of 21 and who has no prior convictions could reasonably be expected to be sentenced to three years of imprisonment or more. The Court refuted the applicant's argument that this provision was not sufficiently precise. It asserted that foreseeability did not require an exhaustive list of offences which are apt to justify phone interceptions and held that the interpretation of the term serious contained in the law gave citizens sufficient information as to the circumstances in which phone interceptions could be authorized (para 160).

As may be inferred from the above judgment, foreseeability of phone interceptions may also be ensured by listing all offences for the investigation of which the interception of communication may be ordered.

Specifying the crimes – not matter in which way – only satisfies the requirement that sufficient safeguards be built in the law if it curbs the number of potential phone interceptions effectively. In *Iordachi v Moldova*, the Court dealt with the Moldovan 'Operational Investigative Activities Act' of 1994. This act provided that phone interceptions could be undertaken for the investigation of serious, very serious and exceptionally serious offences and the Criminal Code contained a definition of these terms. While the category of crimes liable to give rise to an interception was thus clearly defined, the Court criticized that 'more than half of the offences provided for in the Criminal Code fall within the category of offences eligible for interception warrants' (para 44).

B. Georgian legislation

Article 9 (2) of Law on Operative Investigation Activity states that "holding operative-investigation activity that restricts the right of privacy of telephone conversation or other communication by any other means is acceptable only on the basis of judicial permission and the resolution of a prosecutor **or** the activities are permitted on the basis of a written motion of the person that is the victim of the offence, **or** in case there is evidence of a crime generally punishable by criminal legislature with more than two years imprisonment..."

This norm allows concluding that interception in Georgia may be requested when there is**:**

- a resolution of the prosecutor

or

- a written motion of the victim of any offence

or

- there is an evidence of a crime generally punishable by criminal legislature with more than 2 years imprisonment. There are 376 crimes defined in the Criminal Code – 211 of them have more than 2 years imprisonment as punishment; 88 have less or other means of punishment; 77 crimes are generally punished with imprisonment of less than 2 years but in certain circumstances the punishment can be more than 2 years' imprisonment.

This means that a telephone interception (in urgent and non-urgent cases) can be requested for any offence provided by the Criminal Code when there is a resolution of the prosecutor, in the vast majority of the crimes when there is a motion of the victim or alternatively for any crime punishable by criminal legislature with more than two years imprisonment. This is a far reaching provision that allows virtually for any crime or a vast majority of crimes to be subject to interception contrary to the human rights standards developed under the case-law of the ECtHR. In above cited case *Iordachi and Others v. Moldova* the Court criticized the fact that the domestic law providing for phone interceptions could be undertaken for the investigation of "more than half of the offences provided for in the Criminal Code". This aspect was found by the ECtHR as problematic. Applying the same rationale to the Georgia law, it means that the current setting of the legal framework regarding the categories of crimes is problematic.

The ECtHR emphasized that the condition of foreseeability does not require states to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences. (*Kennedy v. UK*, para., 159) Under the current legal settings the Georgian legislation actually permits interception to be used for all or a vast majority of crimes provided by the Criminal Code. Usually interception is used only for criminal offences considered as serious and for which a certain level of punishment applies (e.g. imprisonment for 5 years and more). The Georgian legislation must take into account the standards with regard to the nature of the offence which may give rise to interception order and formulate the relevant provision accordingly.

C. Best practices
Germany (the law enumerates the categories of crimes)

Section 100a of the Criminal Procedure Code puts forward certain conditions regarding interception of telecommunications, namely it states that "(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if ...
2. *the offence is one of particular gravity* in the individual case ...
(2) *Serious criminal offences* for the purposes of subsection (1), number 1, shall be:
1. pursuant to the Criminal Code:
a) crimes against peace, high treason, endangering the democratic state based on the rule of law, treason and endangering external security pursuant to sections 80 to 82, 84 to 86, 87 to 89a and 94 to 100a;
b) bribery of a member of parliament pursuant to section 108e;

c) crimes against the national defence pursuant to sections 109d to 109h;
d) crimes against public order pursuant to sections 129 to 130;
e) counterfeiting money and official stamps pursuant to sections 146 and 151, in each case also in conjunction with section 152, as well as section 152a subsection (3) and section 152b subsections (1) to (4);
f) crimes against sexual self-determination in the cases referred to in sections 176a, 176b, 177 subsection (2), number 2, and section 179 subsection (5), number 2;
g) dissemination, purchase and possession of pornographic writings involving children and involving juveniles, pursuant to section 184b subsections (1) to (3), section 184c subsection (3);
h) murder and manslaughter pursuant to sections 211 and 212;
i) crimes against personal liberty pursuant to sections 232 to 233a, 234, 234a, 239a and 239b;
j) gang theft pursuant to section 244 subsection (1), number 2, and aggravated gang theft pursuant to section 244a;
k) crimes of robbery or extortion pursuant to sections 249 to 255;
l) commercial handling of stolen goods, gang handling of stolen goods and commercial gang handling of stolen goods pursuant to sections 260 and 260a;
m) money laundering or concealment of unlawfully acquired assets pursuant to section 261 subsections (1), (2) and (4);
n) fraud and computer fraud subject to the conditions set out in section 263 subsection (3), second sentence, and in the case of section 263 subsection (5), each also in conjunction with section 263a subsection (2);
o) subsidy fraud subject to the conditions set out in section 264 subsection (2), second sentence, and in the case of section 264 subsection (3), in conjunction with section 263 subsection (5);
p) criminal offences involving falsification of documents under the conditions set out in section 267 subsection (3), second sentence, and in the case of section 267 subsection (4), in each case also in conjunction with section 268 subsection (5) or section 269 subsection (3), as well as pursuant to sections 275 subsection (2) and section 276 subsection (2);
q) bankruptcy subject to the conditions set out in section 283a, second sentence;
r) crimes against competition pursuant to section 298 and, subject to the conditions set out in section 300, second sentence, pursuant to section 299;
s) crimes endangering public safety in the cases referred to in sections 306 to 306c, section 307 subsections (1) to (3), section 308 subsections (1) to (3), section 309 subsections (1) to (4), section 310 subsection (1), sections 313, 314, 315 subsection (3), section 315b subsection (3), as well as sections 361a and 361c;
t) taking and offering a bribe pursuant to sections 332 and 334;
2. pursuant to the Fiscal Code:
a) tax evasion under the conditions set out in section 370 subsection (3), second sentence, number 5;
b) commercial, violent and gang smuggling pursuant to section 373;
c) handling tax-evaded property as defined in section 374 subsection (2);

3. pursuant to the Pharmaceutical Products Act:
criminal offences pursuant to section 95 subsection (1), number 2a, subject to the conditions set out in section 95 subsection (3), second sentence, number 2, letter b;
4. pursuant to the Asylum Procedure Act:
a) inducing an abusive application for asylum pursuant to section 84 subsection (3);
b) commercial and gang inducement to make an abusive application for asylum pursuant to section 84a;
5. pursuant to the Residence Act:
a) smuggling of aliens pursuant to section 96 subsection (2);
b) smuggling resulting in death and commercial and gang smuggling pursuant to section 97;
6. pursuant to the Foreign Trade and Payments Act:
criminal offences pursuant to section 34 subsections (1) to (6);
7. pursuant to the Narcotics Act:
a) criminal offences pursuant to one of the provisions referred to in section 29 subsection (3), second sentence, number 1, subject to the conditions set out therein;
b) criminal offences pursuant to section 29a, section 30 subsection (1), numbers 1, 2 and 4, as well as sections 30a and 30b;
8. pursuant to the Precursors Control Act:
criminal offences pursuant to section 19 subsection (1), subject to the conditions set out in section 19 subsection (3), second sentence;
9. pursuant to the War Weapons Control Act:
a) criminal offences pursuant to section 19 subsections (1) to (3) and section 20 subsections (1) and (2), as well as section 20a subsections (1) to (3), each also in conjunction with section 21;
b) criminal offences pursuant to section 22a subsections (1) to (3);
10. pursuant to the Code of Crimes against International Law:
a) genocide pursuant to section 6;
b) crimes against humanity pursuant to section 7;
c) war crimes pursuant to sections 8 to 12;
11. pursuant to the Weapons Act:
a) criminal offences pursuant to section 51 subsections (1) to (3);
b) criminal offences pursuant to section 52 subsection (1), number 1 and number 2, letters c and d, as well as section 52 subsections (5) and (6).

Republic of Moldova (the law was changed so as to satisfy ECtHR standards after *Iordachi v. Moldova* judgment, the legislature lists offences that may be subject to interception)

Article 132^8 (2) of the Criminal Procedure Code - The provisions of paragraphs. (1) applies exclusively to criminal prosecution which have as their object or try those on which no data or evidence of the commission of the offenses set forth in the following articles of the Criminal Code: Art. 135-137, art. 138 para. (2) and (3), art. 139, art. Article 140. (3) and (4), art. 1401 par. (3) and (4), art. 141 par. (2), art. 142 para. (2) and (3), art. 143-145, art. 151 para. (2) and (4), art.

164 para. (2) and (3), art. 165, art. 166 para. (2) and (3), art. 171 para. (2) and (3), art. 186 para. (2) lit. c), para. (3) - (5), art. 187 para. (2) lit. f), para. (3) - (5), art. 188 para. (2) lit. f), para. (3) - (5), art. 189 para. (3). a), d) and f), para. (4) - (6), art. 190 para. (3) - (5), art. 191 para. (5), art. 206, art. 216 para. (3), art. 2171 par. (4), art. 2174 par. (3), art. 236 para. (2), art. 243 para. (3), art. 248 para. (5), art. 278 para. (2) - (6), art. 2781, art. 279, art. 2791 par. (3) and (4), art. 280 para. (3), art. 283, art. 284, art. 292 para. (2), art. 295 para. (6), art. 2951 par. (3), art. 324, art. 325, art. 326 para. (3), art. 328 para. (3), art. 333, art. 334, art. 337-340. Component list of offenses is exhaustive and may be amended only by law.

United Kingdom (legislation provides for sufficient details regarding the nature of crimes, according to ECtHR this provision satisfies the condition of foreseeability - the law was reviewed in *Kennedy v. UK*)

According to section 5 (3) of Regulation of Investigatory Powers Act (RIPA) "Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary
(a)in the interests of national security;
(b)for the purpose of preventing or detecting serious crime;
(c)for the purpose of safeguarding the economic well-being of the United Kingdom; or
(d)for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement".

All these terms was found by ECtHR to be sufficiently clearly defined in RIPA itself or other laws as to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures. (*Kennedy v. UK* para. 159)

Categories of persons

A. ECtHR standards
The law has also to *define the category of persons liable to be targeted by phone interceptions.* In *Iordachi v Moldova*, the ECtHR noted that the language of the law, which prescribed that 'suspects, defendants or other persons involved in a crime' not indicate with sufficient clarity, which category of persons might be affected by phone interceptions. In particular, the Court pointed out that there was no definition of the term 'other persons involved in a criminal offence' (too large category) (para 44).

By way of contrast, the ECtHR found the German G 10, the law which governs phone interceptions by German intelligence agencies, to be compliant with the requirements of article 8 ECHR (*Klass v Germany*, para 51 read with para 17). Pursuant to this law, persons who could be

targeted by interceptions were "the suspect or such other persons who are, on the basis of clear facts *(bestimmter Tatsachen*), to be presumed to receive or forward communications intended for the suspect or emanating from him or whose telephone the suspect is to be presumed to use".

B. Georgian law

Article 2 of the law enumerates the aims of the special measures from which, if interpreted, one could guess categories of persons that could be subjected to interception:

- Investigating, stopping or preventing a crime
- Identifying the person who prepares, who commits or has committed a crime or other illegal activity;
- Searching for and bringing persons before relevant state body, who are evading from investigation, fleeing from a determined criminal sanction
- Searching and finding the property lost by a crime
- Searching for a missing person
- Collecting necessary factual evidences for criminal cases
- Identifying the person committing a crime.

According to the Article 6 (1) of the same law, carrying out any operative-investigation activities for any other purposes is forbidden. Therefore, interception on anyone who is not directly related to the above mentioned purposes is forbidden.

At the same time, Article 3 (11) of the Code of Criminal Procedure provides for a reasonable suspicion test *i.e.* the existence of the facts or information which in consideration with the circumstances of a case would be sufficient for an objective person to conclude that a person is probably a perpetrator of a crime. This provision read together with the Law on Operative Investigation Activity allows to conclude that persons satisfying the reasonable suspicion test might fall under the category of persons that might be subjected to telephone interception. However, when it comes to third persons *i.e.* those against whom there is no reasonable suspicion that they have committed a crime but might be somehow related to the case, the law is silent. Thus, there is a real risk of indiscriminate capturing of big amounts of communications. The categories of persons liable to have their correspondence intercepted should be limited and clearly defined in the law.

C. Best practices

Germany (legislation specifically indicates which categories of persons may be intercepted)

Section 100a of the Criminal Procedure Code states that "(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if

1. certain facts give rise to the suspicion that a person, either as *perpetrator or as inciter or accessory*, has committed a serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence".

Republic of Moldova (the law was changed so as to satisfy ECtHR standards after *Iordachi v. Moldova* judgment, the legislature clearly provides for categories of persons liable to have their phone subjected to interception)

Article 132^8 (3) of the Criminal Procedure Code states "May be subject to interception and recording of communications, *a suspect, accused, or persons contributing* in any way to the commission of offenses referred to in par. (2) and for which there are data that can reasonably lead to a conclusion that these people receive or transmit to the suspect, accused or defendant information relevant to the criminal case."

Switzerland

Section 66 (1) of the Criminal Procedure Act provides "The investigating judge may order monitoring of the *accused's or suspect's* postal correspondence and telephone and telegraphic telecommunications... if (b) specific facts cause the person who is to be monitored to be *suspected of being a principal or accessory* in the commission of the offence"... paragraph (1) bis. states that "Where the conditions justifying the monitoring of the accused or suspect are satisfied, *third parties* may also be monitored if specific facts give rise to the *presumption that they are receiving or imparting information intended for the accused or suspect* or sent by him ... The telephone connection of third parties may be monitored at any time if there are reasons to suspect that it is being used by the accused."

Interception to be requested base on the existence of a reasonable suspicion

A. ECtHR standards

In addition, to the requirement that ECtHR put forward related to the express provision of categories of persons liable to telephone interception, taking into consideration that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a *reasonable suspicion* that the person is involved in serious criminal activity should be taken as a basis for authorizing it. Legislation must elaborate on the degree of reasonableness of the suspicion against a person. In *Iordachi and Others v. Moldova* the ECtHR noted that the relevant national legislation did not elaborate on the degree of reasonableness of the suspicion against a person for the purpose of authorising interception nor did it contain additional safeguards, for example the provision according to which interception should take place only when it is otherwise impossible to achieve the aims.

B. Georgian legislation

The Law on Operative Investigation Activity does not make an express reference to the degree of reasonableness of the suspicion against a person who may be liable to interception. As mentioned above, Article 3 (11) of of the Code of Criminal Procedure provides for a reasonable suspicion test to be applied for conducting an investigatory action (including wiretapping). Even though, the

mentioned paragraph while defining the reasonable suspicion test does imply its application to investigatory actions, including wiretapping, it is better if the Law on Operative Investigation Activity expressly specifies that the test directly applies to wiretapping, like it does in other investigatory actions, such as the search and seizure (Article 119).

C. Best practices

Germany

Section 100a (1) 1. of the Criminal procedure Code stipulates that "telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if

1. certain *facts give rise to the suspicion* that a person, either as perpetrator or as inciter or accessory, has committed a serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence".

Duration

A. ECtHR standards

Protection against arbitrary or excessive use of phone interceptions requires that the law, on which the phone tapping is based, limits the duration of the measure. The ECtHR has not established a general maximum duration for phone interceptions. In *Association for European Integration and Ekhimdziev v Bulgaria*, it held a maximum duration of two months with a possibility of extension to up to six month on the basis of a fresh application and warrant to be in accordance with the Convention. In *Weber and Saravia v Germany*, it found an interception of up to three months with the possibility of renewal for another three months to be in compliance with article 8 ECHR. (para 98) In *Kennedy v UK*, it ruled that the British 'Regulation of Investigatory Powers Act, which foresees interceptions for a period of six months with the possibility of renewal satisfied the requirements for necessary safeguards. On the other hand, the Court criticized in *Iordachi v Moldova* that the relevant provisions of Moldovan law limited the duration of phone interceptions to six month, but allowed for renewals (para 45).

B. Georgian legislation

In regard to duration of any telephone tapping the law has to stipulate a period after which an interception warrant will expire and, second, the conditions under which a warrant can be renewed.

The Law on Operative Investigative Activity is silent in regard to the initial period after which an interception warrant will expire. This was rectified by a recent recommendation of the Supreme Court of Georgia. According to the Recommendation of the Supreme Court of Georgia from 4 January 2013, a competent court shall determine the duration of the phone interception for 1 month, which is a reasonable term for collecting evidences.

The content of the recommendation is in line with ECtHR standards, however taking into account that Supreme Court's recommendations do not have an obligatory power, and in the light of the fact that according to Strasbourg Court minimum safeguards should be set out in statute law, it is necessary that the content of the mentioned recommendation is reflected in the relevant legislation. Monitoring measures should remain in force for a fairly short maximum period of time and has to be discontinued immediately once the conditions set out in the monitoring order are no longer fulfilled or the measures themselves were no longer necessary.

According to Article 8 (11) - (4) of the Law on Operative Investigation Activity the duration of the operative investigative activity can be extended for 6 months and then renewed to 9 and maximum to 12 months. However, the same provision excludes from its coverage phone interception, which is regulated by the general rules of Article 7 (2) letter „ơ" and „o ". That means that an extension of an interception can be only authorized by a judge. However, the law does not provide a concrete period of time for an extension. The above mentioned Recommendation of the Supreme Court states that extension shall only be granted in exceptional cases, if the necessity is demonstrated on the basis of evidence but also fails to provide for a concrete period and limits of an extension. It is important that the law expressly provides for the limits of the duration of a surveillance measure in order to protect against arbitrary or excessive use of phone interceptions. Also taking into consideration that the recommendations of the Supreme Court do not bear a mandatory character its indications related to the exceptionality of the renewal of an interception should be embedded in the law.

C. Best practices

Germany

Article Section 100b of the Criminal procedure Code regulates issues related to an order to intercept telecommunications and states regarding to the duration that "The order shall be limited to a maximum duration of *three months*. An extension by not more than *three months* each time shall be admissible if the conditions for the order continue to exist, taking into account the information acquired during the investigation."

Republic of Moldova (the law was changed so as to satisfy ECtHR standards after *Iordachi v. Moldova* judgment)

Article 20 (7) "The special investigative measures may be disposed for a period of *30 days* and may be extended based on a reasoned up to 6 months. Each extension of the special investigative measure may not exceed *30 days*. If the period of authorization to carry out special investigative measure was extended up to *6 months*, repeated authorization of the special investigative measure on the same basis and on the same subject is prohibited, except […] when new circumstances appear and cases of investigating the facts regarding organized crime and terrorist financing".

Interception should be a last resort measure

A. ECtHR standards

In addition to the above enumerated guarantees the human rights rationale dictates that interception should be used as a last resort measure when all other classical means are unsuccessful or when there is little or no probability of revealing a crime without the use of interception.

B. Georgian legislation

There is no such provision in the Law on Operative Investigation Activity. Article 20 of the law states that as far as telephone interception is concerned a restriction of the constitutional rights and freedoms can be allowed only by the motivated decision of the court. Though this is an important safeguard, the Georgia legislation does not expressly limit the use of interception and virtually it could be also used even in cases when other less intrusive methods are available.

C. Best practices

Germany

Section 100a (3) of the Criminal Procedure Code allows telecommunications interception only when "other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success".

Switzerland

Section 66 (1) c) of the Criminal Procedure Act provides that "The investigating judge may order monitoring of the accused's or suspect's postal correspondence and telephone and telegraphic telecommunications if ... without interception, the necessary investigations would be significantly more difficult to conduct or if other investigative measures have produced no results".

The procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communication the data to other parties

A. ECtHR standards

According to ECtHR (*Weber and Saravia)* the procedure to be followed for examining and using the data obtained needs to be regulated in detail. In particular, the law should lay down limits and precautions concerning the transmission of data to other authorities. Also the law should "lay down limits on the age of information held or the length of time for which it may be kept" (see *Rotaru v. Romania*, para 57).

B. Georgian legislation

Georgian legislation provides several provisions on the use of data obtained through wiretapping.

According to the Article 11(1) of the Law on Operative Investigation Activity, material obtained through operative investigation activities can be used for investigatory or other measures provided in the Criminal Procedural Code (e.g. search and seizure, pre-trial detention, bail, etc.) and for prevention of crimes. Article 5, further states that operative investigative activities are highly classified and can only be accessed by the persons empowered in accordance with this law. The prosecutor can declassify materials obtained for submitting them as evidence, provided that vital interests of a state, foreign relations, intelligence, economy and public order is not harmed. It is prohibited to use such materials for scientific or any other reasons within 25 years when it was obtained.

When it comes to storing the data, the law under Article 7 (7) states that operative investigative activity is documented by written protocol which reflects details of use of technical means during the surveillance and the protocol is stored together with the material obtained. Unfortunately, the law is silent regarding the term, concrete procedures and conditions regarding the storing of the obtained information during the interception. In addition, it could be assumed that in practice such information could be kept for many years, since Article 5 (3) of the Law on Operative Investigation Activity states that after 25 years material obtained during an operative investigative activity could be used for scientific or any other reasons. This could raise concern, especially in the light of the fact that the current law lacks many of the human rights safeguards. It has to be noted that in *Association "21 December 1989" v. Romania*, the ECtHR found the availability after 16 years of information gathered as a result of the applicant's phone interception as being problematic in the light of the lack of guarantees in the domestic law against abuse.

With regard to the precautions to be taken when communication the data to other parties it has to be mentioned that **t**he Georgian legislation protects the private life of the persons including the secrecy of the private conversations, correspondence and communication. According to Article 5 (2) of the Law on Operative Investigation Activity disclosure of the operative investigation information, to which person had access due to his or her work responsibilities or other duties will result in his criminal liability for disclosure of state secrets. Disclosure of state secret is provided in Article 313 of the Criminal Code of Georgia and is punishable by prison sentences ranging from five to fifteen years in length, by deprivation of the right to occupy a position or pursue a particular activity for the term not in excess of three years. Also the illegally obtaining, storing or dissemination of personal or family secrets is punishable, as is the illegal interception of private conversation or disclosure of the information (Articles 157 - Disclosure of Personal or Family Secrets , 158 - Disclosure of Secret of Private Conversation of the Criminal Code).

Nevertheless, the law does not provide any procedure concerning the transmission of data between different authorities, neither it includes precise regulations specifying the manner of screening the intelligence obtained through surveillance, or the procedures for preserving its integrity and confidentiality and the procedures for its destruction.

C. Best practices

Germany

Criminal Procedure Code:

Section 98a

[Automated Comparison and Transmission of Personal Data]

(1) ... where there are sufficient factual indications to show that a criminal offence of substantial significance has been committed

1. relating to the illegal trade in narcotics or weapons or the counterfeiting of money or official stamps,
2. relating to national security (sections 74a, 120 of the Courts Constitution Act),
3. relating to offences which pose a danger to the general public,
4. relating to endangerment of life and limb, sexual self-determination or personal liberty,
5. on a commercial or habitual basis, or
6. by a member of a gang or in some other organized way,

personal data relating to individuals who manifest certain significant features which may be presumed to apply to the perpetrator may be automatically matched against other data in order to exclude individuals who are not under suspicion or to identify individuals who manifest other significant characteristics relevant to the investigations. This measure may be ordered only where other means of establishing the facts or determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult.

(2) For the purposes of subsection (1), the storing agency shall extract from the database the data required for matching purposes and transmit it to the criminal prosecuting authorities.

(3) Insofar as isolating the data for transmission from other data requires disproportionate effort, the other data shall, upon order, also be transmitted. Their use shall not be admissible.

(4) Upon request by the public prosecution office, the storing agency shall assist the agency effecting the comparison.

Section 98b

[Competence; Return and Deletion of Data]

(1) Matching and transmission of data may be ordered only by the court and, in exigent circumstances, also by the public prosecution office. Where the public prosecution office has made the order, it shall request court confirmation without delay. The order shall become ineffective if it is not confirmed by the court within three working days. The order shall be made in writing. It shall name the person obliged to transmit the data and shall be limited to the data and comparison characteristics required for the particular case. The transmission of data may not be ordered where special rules on use, being provisions under Federal law or under the corresponding *Land* law, present an obstacle to their use. Sections 96 and 97, and Section 98 subsection (1), second sentence, shall apply *mutatis mutandis*.

[...]

(3) Where data was transmitted on data media these shall be returned without delay once matching has been completed. Personal data transferred to other data media shall be deleted without delay once it is no longer required for the criminal proceedings.
(4) Upon completion of a measure pursuant to Section 98a, the agency responsible for monitoring compliance with data protection rules by public bodies shall be notified.

Section 98c
[Comparison of Data to Clear Up a Criminal Offence]
In order to clear up a criminal offence or to determine the whereabouts of a person sought in connection with criminal proceedings, personal data from criminal proceedings may be automatically matched with other data stored for the purposes of criminal prosecution or execution of sentence, or in order to avert danger. Special rules on use presenting an obstacle thereto, being provisions under Federal law or under the corresponding *Land* law, shall remain unaffected.

Circumstance under which the recordings or tapes may or must be erased or destroyed

A. ECtHR standards
According to ECtHR, legislation on secret surveillance should set out in detail the procedure for the destruction of data obtained by means of monitoring. In *Weber and Saravia v. Germany* the ECtHR found that the procedure was detailed enough and the authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office.

B. Georgian legislation
According to Article 6 (4) of the Law on Operative Investigation Activity, collected data, which does not relate to the criminal activities of the person, but includes compromising information, should not be made public or used in any way against the person. Such information should not be stored and must be destroyed immediately, about this the minister of justice, or the chief prosecutor, also the chief or the deputy, chief of the supervisory body should be informed.

Though this is an important safeguard it has a limited application, since according to the above mentioned article only information which is not related to the criminal activity and has a compromising character must be destroyed. This provision does not oblige the competent body to delete any other type of information collected during interception which proved to be unrelated to the criminal activity. This runs the risk that personal data and information may be stored though not related in any way to the crime. In addition, the legal norm under review does not impose the obligation that destroying such data should be documented accordingly and introduces only the

duty to inform the minister of justice/chief prosecutor and supervisory body. Though the latter duty is an important safeguard against abuse a duty to document should be introduced as well.

In addition, the law seems to be completely silent on the destruction of collected data in general after for example proceedings are finalized or after the completion of a certain period of time.

C. Best practices

Germany

Section 100a (4) of the Criminal Procedure Code states that "If there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired through a measure pursuant to subsection (1), the measure shall be inadmissible. Information concerning the core area of the private conduct of life which is acquired during a measure pursuant to subsection (1) shall not be used. Any records thereof shall be deleted without delay. The fact that they were obtained and deleted shall be documented."

Precautions have to be taken to protect privileged communication between attorney and client

A. ECtHR standards

The legal basis for phone interceptions *has to provide rules ensuring that information falling under the lawyer-client privilege is not intercepted.* The right to legal assistance by a lawyer is a cornerstone of democratic societies. Anybody interested in consulting a lawyer should have the possibility to do so under conditions which allow for a free exchange of information (*Campbell v UK*, para 46). This right would lose value if persons conferring with their lawyers would have to fear that the conversation might be intercepted. Therefore, measures have to be taken to secure the protection of privileged conversations. Including in the law a rule to the effect that conversations between lawyers and their clients is not tapped is not a sufficient means to safeguard the confidentiality of conversations between lawyers and their clients. It also has to become clear which steps are taken to ensure that this rule is respected in practice (*Iordachi v Moldova*, para 50). In *Kopp v Switzerland*, the EHtHR found the respondent state in violation of article 8 ECHR, because the law and practice of phone tapping did not ensure that the exchange of information falling under the lawyer-client privilege was protected. While Swiss law provided that phones of lawyers were not to be tapped, conversations between lawyers and clients were intercepted. The Swiss government argued that according to Swiss law certain pieces of information exchanged between lawyers and their clients were not protected by lawyer-client confidentiality (this concerned for example information regarding the handling of funds). Therefore, the Swiss authorities tried to distinguish between privileged information, which did not become part of the case file, and not privileged information, which could be added to the case file and considered in court. The person tasked to sort between these two types of information was a lawyer working with the post department, which was state-owned and in charge of telecommunications at the material time. The Court criticized this arrangement as generally not sufficiently clear with regard

to procedure to distinguish privileged information from non-privileged information and stated that '*in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence.'* . As an example to the contrary, the ECtHR approved of the precautions taken in Dutch law in *Aalmoes v The Netherlands*. Dutch law distinguished whether the lawyer was a suspect or a third-party. In the instance the lawyer was a suspect, his phone could be tapped, but material protected by the lawyer client privilege had to be sorted out. A representative of the bar association was involved in the decision which material was protected. In case the lawyer was not a suspect, his phone could not be intercepted. Communications falling within the ambit of the lawyer-client privilege, which were intercepted (for example because the suspect in a case called a lawyer) had to be screened by a prosecutor. The prosecutor ordered that privileged information be destroyed. Only information which was not privileged could be taken to the file upon approval by a judge.

B. Georgian legislation

The Law on Operative Investigation Activity 16 (3) and the Code of Criminal Procedures (Article 43) declares that lawyer-client communication is confidential. Article 16 (3) States that investigation bodies cannot violate the right of confidentiality of attorneys and others, who are bound to keep professional information confidential.

Though the Georgian legislation guarantees the attorney-client communications, it does not provide for any procedure which would give substance to the above mentioned guarantee. In *Iordachi and Others v. Moldova* the ECtHR criticised a similar provision and noted that it was struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted (para. 50). The Georgian legislation similarly does not contain any rules that would give substance to the established guarantee. There is a need for clear rules that would reflect which concrete steps are to be taken to ensure that this guarantee is respected in practice and does not remain only a theoretical guarantee.

Oversight mechanism

A. ECtHR standards

According to human rights standards there have to be control mechanisms to ensure that the law is complied with. Also the oversight has to be in line with generally accepted democratic principles and has to be carried out by an authority independent from the one which carries out the measure.

B. Georgian legislation

According to Article 12 of the Operative - Investigation Activity the following entities have the exclusive competence to undertake the conduct of secret surveillance, including wiretapping:

operative and investigative agencies and units of the Ministry of Internal Affairs; operative bodies of the State Special Security Service; operative agencies and investigative units of the Ministry of Finance; investigators of investigative unit and security service of the penitentiary and Deprivation of Liberty Institution of the Ministry of Corrections and Legal Assistance; operative, investigative and intelligence units of the Ministry of Defense; operative units of the Intelligence Service; investigators of the Prosecutor's Office; investigators and staff of the Operations Division of the Ministry of Justice.

The control and supervision of the secret surveillance conducted by the above mentioned entities is realized by the chief of the operative-investigation organization who is personally responsible, the legality of the activities is controlled by the minister of justice and the prosecutors under his or her control. With regard to the court control, the judge should give permit for telephone interception, as far as it restricts constitutional rights and freedoms.

The control and review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. The initial control under Georgian legislation is entrusted in judiciary, which is considered to be under ECtHR standards as an effective control (*Klass and Others v. Germany* para. 55) because judicial control offers the best guarantees of independence, impartiality and proper procedure. However, the law makes no provision for acquainting the judge with the results of the surveillance and does not required him to review whether the requirements of the law have been complied with.

The subsequent control is entrusted in the chief of the operative-investigation organization who is personally responsible, the legality of the activities is controlled by the minister of justice and the prosecutors. However the detailed manner in which control is effectuated is not set out in the law. The ultimate control and supervision of secret surveillance is invested in the Minister of Justice and the prosecutor's office, entities that are indeed operationally independent from other competent authorities that have the power to conduct operative-investigation measures (though not in the case when interception is conducted by the relevant unit of the of the Ministry of Justice itself), however they are a part of the executive and thus cannot be considered as an independent authority from the one which carries out the measure. The oversight mechanism should be entrusted to an independent authority.

C. Best practices

United Kingdom (final oversight is entrusted in a special Commissioner)

Section 57 RIPA provides that the Prime Minister shall appoint an *Interception of Communications Commissioner*. He must be a person who holds or has held high judicial office. The Commissioner is appointed for a three-year, renewable term. The Commissioner's functions include to keep under review the exercise and performance by the Secretary of State of powers and duties in relation to interception conferred or imposed on him by RIPA; the exercise and performance of powers and duties in relation to interception by the persons on whom such powers

or duties are conferred or imposed; and the adequacy of the arrangements by virtue of which the duty which is imposed on the Secretary of State by section 15. The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State based his decision. Section 58 RIPA places a duty on those involved in the authorisation or execution of interception warrants to disclose to the Commissioner all documents and information which he requires in order to carry out his functions. The Commissioner is required to report to the Prime Minister if he finds that there has been a violation of the provisions of RIPA or if he considers that the safeguards under section 15 have proved inadequate (sections 58(2) and (3) RIPA). The Commissioner must also make an annual report to the Prime Minister regarding the exercise of his functions (section 58(4)). Under section 58(6), the Prime Minister must lay the annual report of the Commissioner before Parliament.

Republic of Moldova (parliamentary oversight)
Article 38 of the Law on Operative Investigation Activities provides for a parliamentary oversight, which is invested in the Commission on National Security, Defence and Public Order. The authority carrying out special investigation activity is obliged to present until January 15 of each next year to the Prosecutor General, a report on the work of special investigation, which will include the following information: a) the number of authorized special investigative measures; b) the number of canceled special investigative measures; c) the results of special investigative measures. The Prosecutor General on the basis of the received reports and available information presents until February 15 of each year, a final report on the operative investigative activities to the Commission on National Security, Defence and Public Order. The Commission may request any additional information on special investigation activities, where it considers that the report is incomplete.