Ivane Javakhishvili Tbilisi State University
Faculty of Law

Journal of Law

№1, 2019

უნივერსიტეტის
გამომცემლობა

UDC(უაკ) 34(051.2)
ს-216

Published by the decision of Ivane Javakhishvili Tbilisi State University Publishing Board

ISSN 2233-3746

Tamar Gegeshidze*

Monitoring of Internet Communications in Criminal Proceedings

The present paper reviews the Georgian Legislation and international standards related to secret investigative actions of obtaining internet communications. Due to rapid development of modern technologies, protection of privacy in the field of electronic surveillance has become the significant challenge. Since the Constitutional Court of Georgia, under the judgement of April 14, 2016 recognized as unconstitutional certain provisions regulating secret investigative actions of obtaining communications in real time, this issue has acquired a special importance in Georgia. Taking into consideration the above mentioned, the aim of the present paper is to discuss the legal standards established by the Constitutional Court of Georgia and amendments into the legislation, to analyze certain problematic issues with regard to monitoring of internet communications and to demonstrate the best international practice developed in this field.

Key words: *Monitoring of internet communications, right to privacy, secret surveillance measures, obtaining communications in real time, secret investigative actions.*

1. Introduction

Information technologies, particularly the internet have brought fundamental changes in the life of society.[1] By allowing large amount of information to be transferred rapidly and with less expense all over the world, the internet has transformed the present capabilities of communication.[2] Internet communication, in terms of application, competes with more traditional methods of communication, such as telephone communication. "There is no actual difference in exchange of information on the phone and on the internet in terms of amount, content, characteristics, kind of exchangeable information between individuals. Moreover, by the rate of usage and consequently, by informative value and the volume of data, internet communication nowadays may be much more informative. Accordingly, uncontrolled access to this field may provoke much more serious interference with privacy and may violate the fundamental rights as a result".[3]

Parallel to the modern technological progress, technical capabilities of state in the field of electronic surveillance are gradually increasing. Electronic communications may reveal the most personal and intimate information on individuals, including their past or future actions. Accordingly, communications represent valuable source of evidence.[4]

---

* PhD Student at Iv. Javakhishvili Tbilisi State University, Faculty of Law.

1 *Wright J.,* Necessary and Inherent Limits to Internet Surveillance, Internet Policy Review, Vol. 2, Issue 3, 2013, 1.

2 *Clough J.,* Principles of Cybercrime, New York, 2010, 135.

3 Judgment №1/1/625, 640 of April 14th, 2016 of the Constitutional Court of Georgia, 55-56.

4 Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 4, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>, [02.04.2019].

Obtaining internet communications and its use in criminal proceedings represents particularly serious interference with the right to privacy established under Article 15 of the Constitution of Georgia, Article 8 of the European Convention (hereinafter – Convention) on Human Rights and Fundamental Freedoms, Article 12 of the Universal Declaration of Human Rights and number of other international legal acts. Due to limitless nature of Internet and increasing development of modern technologies, protection of privacy is no longer a challenge for only one state and has already acquired the global importance. It is also of a great significance that only just a few year ago the problem of "illegal wiretapping" was the subject of public scrutiny in Georgia. Since August 2014, when the parliament of Georgia has adopted a new legislative package related to covert investigative activities, the protection of privacy hasn't lost its significance in process of obtaining information from the means of electronic communication. Additionally, the Constitutional Court of Georgia, under the decision of April 14, 2016, acknowledged certain provisions related to monitoring of internet communications[5] (as well as interception of telephone communications) to be in violation with constitutional standards[6]. In order to execute above-mentioned judgment, some amendments have been made into Georgian legislation on March 22 2017. However, the dispute is still pending to this day in the Constitutional Court. In this dispute plaintiffs consider that the amendments made to the legislation fail to meet the requirements established by Constitutional Court under the judgment of April 14, 2016.[7]

Taking into consideration the abovementioned, the present paper will cover fundamental guarantees of right to privacy in the field of secret surveillance, capabilities of obtaining the internet communications, legal standards established by Constitutional Court and amendments made into Georgian legislation, as well as certain problematic issues related to monitoring of internet communications and international practice.

2. Right to Privacy and its Fundamental Guarantees Related to Secret Investigative Actions

As it has been already mentioned, internet offers unprecedented opportunities to exchange information from any place in the world. Internet communication tools include applications or websites based on modern technology and available to everyone, such as Facebook, Messenger, Skype, WhatsApp, Viber, Gmail, etc. These products differed from each other functionally and technologically, however the availability of modern technologies enabled companies to develop products in such

---

5 In the Decision №1/1/625, 640 of April 14th, 2016 the Constitutional Court discussed the secret investigative actions provided in sub-paragraph "a" (interception of telephone communications) of the first part of Article 143^1 of Criminal Procedure Code of Georgia and sub-paragraph "b" of the first part of the same article. The measure of obtaining real-time internet communication provided in sub-paragraph "b" of the first part of Article 143^1 is referred to as "monitoring of internet communications".

6 Ibid.

7 Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia.

a way that these, and many other applications offer almost similar services to users, such as: internet telephony (VoIP), video call, text and voice messages, photo/video data sharing, etc.

Privacy of communication is protected under the Article 15 of the Constitution of Georgia, which determines the communication protection from undesired participation of third parties.[8] Communication set by wired and wireless communication systems is protected by the constitution.[9] Additionally, both content of communication and communication identifying information are under the protection of right to privacy.[10] Content data includes the messages sent and received via e-mail, content of the internet telephony, text, voice and other digital format messages exchanged through the internet applications and social networks, files sent and received, etc. Identification data of Communication – metadata includes information created or processed as a result of a communication's transmission.[11] This information makes it possible to identify the person with whom the subscriber has communicated, also the means of communication as well as time and place. Besides, this data makes it possible to determine how often the user communicated with certain individuals in a specific period of time (Joined Cases Tele2 Sverige AB and Watson).[12] Metadata generated from internet communication includes internet protocol address (IP address) which has a special evidential value for investigation. This data can be used to identify and locate a person and track their online activities.[13] Such data also includes "to-from information on e-mails, login times and locations",[14] etc.

As it has been already mentioned, obtaining information from the means of electronic communication and its application in criminal proceedings is a serious limitation to privacy. At the same time, privacy is not an absolute right and the state can interfere in exceptional cases considering significant public interests. The state must have the ability to use secret surveillance measures to neutralize the threats from terrorism and other serious crimes; However, its application is only permissible in exceptional cases provided that mentioned measure represents proportional and necessary mean to achieve a legitimate aim (to protect national security, prevent crime or disorder) (Klass and others v. Germany).[15]

---

8 Comment to the Constitution of Georgia, Chapter Two, Citizenship of Georgia, Human Rights and Freedoms, Tbilisi, 2013, 181. The book refers to Article 20 of the old edition of the Constitution of Georgia (in Georgian).

9 Judgment №1/1/625, 640 of April 14th, 2016 of the Constitutional Court of Georgia, 28.

10 Ibid, 61-62. See also Case NC-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and Others, [2014], Court of Justice, 34. Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98-100.

11 *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No. 2, 2015, 54.

12 Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98.

13 Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 18, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/-Session23/A.HRC.23.40_EN.pdf.>, [02.04.2019].

14 *Kerr O. S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014, 384.

15 Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 49.

The European Court follows the principles of legality, legitimate aim and proportionality in cases related to the rights under Article 8 of the Convention. The principle of legality combines the existence of legal basis in domestic legislation and "quality" requirements of law. The latter includes the criteria for "accessibility" and "foreseeability" of the law. The Court has held on several occasions that the reference to "foreseeability" in the context of secret surveillance of communications is not the same as in many other areas. With regards to this particular issue, "foreseeability of law" does not imply the capability of person to foresee when they may be the subject of surveillance from law enforcement authorities and to alter their actions accordingly. Nevertheless, the risk of arbitrariness is evident due to the secret nature of activities by executive bodies. It is therefore essential to have "clear, detailed rules" on secret surveillance measures, especially as the communication interception technology is constantly being advanced (Malone v. United Kingdom, Leander v. Sweden, Valenzuela Contreras v. Spain, Huvig v. France, Association for European Integration and Human Rights and Ekimdzhiev, Kruslin v. France).[16] "The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures" (Malone v. United Kingdom, Roman Zakharov v. Russia).[17] According to the European Court, since the implementation of these measures in practice is not public to its addressee and the whole society, granting of unrestricted discretion to executive bodies or to a judge would be in contrary to the rule of law. Therefore, the scope of this discretion and the manner of its exercise should be regulated with "sufficient clarity" to ensure adequate guarantees against the arbitrary interference (Roman Zakharov v. Russia).[18] Legislation, allowing the interference with private communications, "must specify in detail the precise circumstances in which such interference may be permitted."[19]

The restriction of the right to privacy under Article 8 of the Convention should also be "necessary in a democratic society" (Kennedy v. United Kingdom).[20] In the context of secret surveillance, the European Court noted in a number of cases that in the process of balancing public and private interests the states are granted certain discretion to choose the measures in order to protect national interests. However, because the secret surveillance measures justified with protection of democracy can itself become the reason for undermining democratic foundations, the law must provide sufficient and effective guarantees against arbitrary interference. From this point of view, during the evaluation all circumstances of the case are taken into consideration, such as "the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise,

---

16 Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67; Leander v. Sweden, [1987], ECtHR, (Ser. A.), 51; Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46. Huvig v. France, [1990], ECtHR, (Ser. A.), 32. Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 75; Kruslin v. France, [1990], ECtHR, (Ser. A.), 33.

17 Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67. Roman Zakharov v. Russia, [2015] ECtHR, 229.

18 Roman Zakharov v. Russia, [2015] ECtHR, 230.

19 General Comment No. 16 Article 17 (The right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), Human Rights Committee, 1988.

20 Kennedy v. United Kingdom, [2010] ECtHR, 130, Roman Zakharov v. Russia, [2015] ECtHR, 227.

carry out and supervise them, and the kind of remedy provided by national law" (Klass and others v. Germany, Kennedy v. United Kingdom, Roman Zakharov v. Russia, Weber and Saravia v. Germany).[21] The requirement for "necessary in a democratic society" implies that secret surveillance measures must meet "strict necessity" test, meaning it should be "strictly necessary" on one hand, as a general consideration to ensure the democratic foundations and on the other, to obtain vital information in a specific case (Szabo and Vissy v. Hungary).[22] The principle of proportionality also requires that selected mean of interference should be the least invasive among the means which might achieve the legitimate aim.[23]

It is noteworthy, that Article 15 of the Constitution of Georgia establishes the legal grounds for interfering with the right to privacy of communications. Based on paragraph 2 of this article, restriction of the rights defined in this article is permissible only in accordance with the law in order to ensure national security or public safety, or to protect the rights of others insofar as is necessary in a democratic society, based on a court decision or without a court decision in cases of urgent necessity provided by the law.[24] The procedure for obtaining information from the means of electronic communication for the purpose of investigation is determined by the Criminal Procedure Code of Georgia (hereinafter - the CPCG). Chapter XVI[1] of CPCG defines the standards related to carrying out the secret investigative actions and to the use of information obtained. The measure of real-time collection of internet communication is defined by subparagraph "b" of the first part of Article 143[1] of the CPCG. Namely, according to this provision, one of the types of secret investigative actions include removal and recording of information from a communications channel (by connecting to the communication facilities, computer networks, line communications and station devices), computer system (both directly and remotely) and installation of respective software in the computer system for this purpose.[25]

3. Capabilities of Obtaining Internet Communications

---

[21] Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 49-50; Kennedy v. United Kingdom, [2010] ECtHR, 153; Roman Zakharov v. Russia, [2015] ECtHR, 232. Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 106.

[22] Szabo and Vissy v. Hungary, [2016] ECtHR, 73.

[23] CCPR General Comment No. 27: Article 12 (Freedom of Movement), UN Human Rights Committee, 02.11.1999, 11-16, Indicated: Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30.06.2014, 9, <https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc>, [27.03.2019]; Also see: International Principles on the Application of Human Rights to Communications Surveillance, <https://en.necessaryandproportionate.org/text>, [02.04.2019].

[24] Constitution of Georgia, Article 15, Departments of the Parliament of Georgia, 31-33, 24/08/1995.

[25] Criminal Procedure Code of Georgia, sub-paragraph "b" of the first part of article 143[1], <www.matsne.gov.ge>, [02.04.2019]

Due to the nature of covert investigative actions and secrecy of these measures, the detailed information on the means used by the states to intercept the online communications, is often hidden from public. However, the various global sources mention main methods used by law enforcement bodies. For example, in the report of UN Special Rapporteur on April 17, 2013 several technical capabilities of obtaining the private communications are highlighted. According to this report, the States have access to a number of different techniques of communications surveillance, for example "by placing a tap on an internet cable relating to a certain location or person, state authorities can also monitor an individual's online activity and obtaining information related to the websites he or she visits."[26] In parallel with the targeted secret surveillance, some States have the capability of mass/total monitoring of internet and telephone communications; "by placing taps on the fibre-optic cables, States can achieve almost complete control of tele - and online communications."[27]

Additionally, to the above-mentioned, practice of obtaining information by law enforcement using the "hacking" technique is under acute discussion and review at international level and scientific circles. As far as it's known, this measure is used by law enforcement bodies of many countries for the purposes of criminal investigation.[28] "Hacking is difficult to define, given the broad scope of activities it covers."[29] For example, according to one of the leading human rights organizations, hacking enables government to gain a remote access to a computer system and, potentially to all data stored on the system.[30] Hacking also allows the real time monitoring of communications.[31] The Federal Constitutional Court of Germany in its judgment of February 27, 2008 concerning the constitutionality of the measure of secret infiltration to computer system explains that secret access to an information technology system makes it possible to monitor its use or to view the storage media, or to control the target system remotely.[32] Additionally, secret infiltration to the computer system may be done in several ways.[33]

---

26 Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 10, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession-/Session23/A.HRC.23.40_EN.pdf>, [02.04.2019].

27 Ibid, 11.

28 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs), Policy Department for Citizens' Rights and Constitutional Affairs, 2017, 42-43, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/-IPOL_STU(2017)583137_EN.pdf>, [03.04.2019]. See also *Winter L. B.,* Remote Computer Searches under Spanish Law: The Proportionality Principle and the Protection of Privacy, Zeitschrift für die Gesamte Strafrechtswissenschaft, Vol.129, No. 1, 2017, 211-212.

29 Encryption and Anonymity Follow-up report, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2018, 7, <https://www.ohchr.org/Documents/-Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>, [02.04.2019].

30 Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 8, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%2-0Hacking%20and%20Surveillance.pdf>, [03.04.2019].

31 Ibid.

32 BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07.

Considerable attention has been paid to the practice of using this technical capability in the aforementioned report of UN Special Rapporteur, where it is highlighted that using such invasive methods as so-called "Trojans (spyware or malware)" constitute a serious challenge to traditional notions of secret surveillance of electronic communications, fall outside of existing legal frameworks and from a human rights perspective, the use of such technologies is extremely intrusive.[34]

It is noteworthy, that usage of communication encryption is increasing by time. Encryption has become standard and necessary tool to ensure data security, as well as protection of private communications. Widespread use of encryption on the internet affects abilities to obtain information by the state.[35] Since the communication through mainstream applications and social networks is sent in encrypted form, local internet service providers are not able to read the data.[36] Accordingly, proven method for access to this information is to request it directly from the companies of web-pages or applications (Facebook, Instagram, etc.). Besides, different types of encryption are available, some companies such as Google or Dropbox keep the data stored in encrypted form and have the technical capability to decrypt the data. Such information may be obtained through this service provider.[37] In case of different types of encryption (such as End-to-end encryption), only the communication parties have technical capability to decrypt (encryption "key") the content of communication on their computers or smartphones and accordingly, the service provides are deprived the ability to read the content.[38] Therefore, obtaining information encrypted through this method is quite challenging for law enforcement agencies.[39] It is noteworthy, that as a general rule, encryption protects only the content of communication and not its identification data such as Internet Protocol address (IP address).[40] Information on the visited websites may be also available in unencrypted form.[41]

---

33 *Vaciago G., Ramalho D. S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings by Digital Evidence and Electronic Signature Law Review, Vol.13, 2016, 88-89, <http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252>, [03.04.2019].

34 Report of the Special Rapporteur On the Promotion and Protection of the Right to Freedom of Opinion and Expression, 17.04.2013, 10, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/-Session23/A.HRC.23.40_EN.pdf>, [02.04.2019].

35 *Swire P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 203.

36 Ibid, 202.

37 *Corn G. S., Brenner-Beck D.,* "Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance", The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S. E.* (eds.), New York, 2017, 334.

38 Ibid, 335.

39 Ibid, 334-335. see *Swire P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 202.

40 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 22.05.2015, 4, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509-585.pdf?OpenElement>, [27.03.2019].

41 Encryption and Anonymity Follow-up Report, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2018, 18, <https://www.ohchr.org/Documents/Issues/-Opinion/EncryptionAnonymityFollowUpReport.pdf>, [02.04.2019].

As it has been already mentioned, private companies hold extensive volume of data. Furthermore, as the flow of electronic information is not restrained by state borders, data may be stored transnationally independent from the territory in which the data was originally collected or in which the data subject is located.[42] Request for information stored with the provider may be made by direct addressing the service provider or through cooperation with state law enforcement bodies under whose jurisdiction falls the service provider.[43] Transnational requests for "voluntary" transfer of information is a standard procedure. This way, the state may avoid formalized procedure of international cooperation.[44] However, request for information directly from service provider may be related to a number of practical difficulties, when the service provider is under the jurisdiction of a foreign state. The requesting state does not have the legal authority to force a company founded within foreign jurisdiction to cooperate and provide information required. Consequently, this cooperation is usually based on a voluntary basis.[45]

Thus, different ways of obtaining internet communication are available for the purpose of investigation. In order to better understand the basic possibilities of obtaining internet communications in criminal proceedings, in parallel with capability of obtaining information in real time, issues related to request information stored with service providers have been also discussed.

4. Standards Established by the Constitutional Court of Georgia and Amendments Made into the Legislation

The Constitutional Court of Georgia, under the judgement of April 14, 2016 recognized as unconstitutional the provision of Georgian law "on electronic communications", under which the State Security Service, the agency responsible for execution of secret investigative actions, had been granted an authority for technical capability to "obtain information in real time from physical lines of communication and their connectors, mail servers, base stations, base station equipment, communication networks and other communication connectors, and for this purpose, to install, where necessary, a lawful interception management system and other appropriate equipment and software free of charge at said communication facilities". The constitutional court acknowledged as unconstitutional not the institute for obtaining real-time communication, but only the authorization of the State Security Service - agency "responsible for the investigation" and "professionally interested" with this power.[46]

---

42 *Haase A., Peters E.,* Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance, International Data Privacy Law, Vol. 7, No. 2, 2017, 126.

43 Ibid.

44 Ibid, 130.

45 Ibid, 130-131.

46 Judgment №1/1/625, 640 of April 14th, 2016 of the Constitutional Court of Georgia.

One of the arguments of non-constitutionality of provisions in the judgement is the circumstance that the legislation did not envisage the right of personal data protection inspector[47] to carry out "full and comprehensive inspection" of the technical infrastructure of obtaining real time information; therefore, arbitrariness and illegality of the body responsible for data processing is not excluded in this process.[48]

As a result of the proceedings in the Constitutional Court it is confirmed that the state authority had the possibility to have the "so-called permanent connection system with internet service providers". It is also confirmed that "they have this apparatus in large companies". However, as it appeared, this system is ineffective and in practice they use "so-called infecting technique" (secret virus installation). "In particular, according to the witness: Although we have this apparatus in a number of large companies to obtain real-time information, this system is not effective, that's why real time internet surveillance system architecture has not been set up... ."[49]

The Constitutional Court considered that "disputed provisions do not separate from each other which technical means should be used by the authorized body for secret investigative actions, which seemed to imply that for monitoring of internet communications it was applicable to use lawful interception management system, as well as other appropriate apparatus and software tools". At the same time according to explanation of State Security Service representative it was ascertained that only the "other appropriate apparatus and software tools" provided by disputed provisions had been used in relation to the internet. According to the Court, as the "information is kept secret" and "audit of those technical means" used for obtaining internet communications is "impossible even on minimal level", "it is not apparent, which apparatus and software tools are used by the state. Therefore, it is impossible to supervise this process and, consequently there is a risk of violation of the rights itself."[50] According to the Court, the state should not be equipped with "completely uncontrolled space, where nobody will ever know what kind of technical means are being utilized and most importantly, whether constitutional requirements are protected or not."[51] Under such circumstances, the only mechanism for the control provided by the law "on Personal Data Protection"[52] - the possibility of inspection, was deemed ineffective.[53]

In order to enforce this judgement, on March 22, 2017 a number of amendments were made into the law about obtaining information from the means of electronic communications and its use in

---

47 As a result of amendments made into the legislation, the position of Personal Data Protection Inspector has been abolished since May 10th 2019 and The State Inspector and the State Inspector Service was deemed to be a successor in title of the Personal Data Protection Inspector. According to the legislation in force at that time, the constitutional court's judgment mentions the position of Personal Data Protection Inspector.

48 Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia, 59.

49 Judgment №1/1/625, 640 of April 14th, 2016 of the Constitutional Court of Georgia, 54.

50 Ibid, 55.

51 Ibid.

52 As a result of amendments made into the legislation, the right of the State Inspector Service in relation to secret investigative actions is currently established in the law "On the State Inspector Service".

53 Judgment №1/1/625, 640 of April 14th, 2016 of the Constitutional Court of Georgia, 55.

criminal proceedings. From this point of view, one of the innovations is establishment of Operative-Technical Agency – a new body, which was founded as a legal entity of public law under the State Security Service and entitled with the power of technical execution of secret surveillance measures.

As a result of amendments, the following ways of obtaining real-time communication have been defined with regards to secret surveillance measures: stationary, semi-stationary and non-stationary technical capability. At the same time, it was determined that covert investigative actions under the subparagraph "b" of the first part of Article 143^1 of CPCG are carried out with stationary, semi-stationary and non-stationary technical capability of obtaining real-time communication.[54]

As it has already been mentioned, empowering operative-technical agency with direct access to telephone and internet communications, as well as capability of copying and storage of metadata, is still under dispute in the Constitutional Court. Within this dispute, the plaintiffs requested to recognize provisions regarding obtaining information in real time as well as the power of copying and retention of metadata as unconstitutional without hearing on the merits. However, under the recording notice of the constitutional court of December 29, 2017 plaintiffs have been refused to recognize abovementioned provisions, as invalid, without hearing on the merits. The Constitutional Court considered that disputable provisions are not identical to the provisions known as unconstitutional under the judgment of the Constitutional Court on April 14, 2016 and the system has been changed significantly through the amendments made into legislation. Therefore, the constitutionality of legislation concerning to obtaining information in real time, including internet communications (also provisions in relation to copying and retention of metadata) will be reviewed on the merits. [55]

As it has already been mentioned, under the judgement of April 14, 2016 unconstitutionality of provisions related to the monitoring of internet communications was conditioned by absence of sufficient external controls. In this regard, the court emphasized the necessity of regulation in the legislation of the inspector's[56] right to inspect the technical means used for electronic surveillance. In this context, the Constitutional Court in the recording notice of December 29, 2017 made a decision on hearing on the merits of disputed provisions upon the grounds of amendments made on March 22, 2017 to the Law of Georgia on "Personal Data Protection"; particularly, an attention has been focused on paragraph 4^1 of Article 35^1 of this Law[57]. According to amendments of March 22, 2017 it was high-

---

54 CPCG, sub-paragraph "b" of part 4 of Article 143^3.

55 Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia According to this recording notice, judges in the court had split opinions related to internet communications, as well as other issues discussed - three judges expressed different opinions and considered that "legislation with regard to Internet communication had not undergone substantial changes that would necessitate a further discussion of hearing on the merits."

56 According to the legislation being in force at that time, the position of "personal data protection inspector" is mentioned in the constitutional court's judgment.

57 It's worth mentioning that as a result of amendments made into the legislation, article 35^1 of the law "On Personal Data Protection" has been annulled and the rights related to inspection which were established in this article were transferred to paragraph 7 of article 18 of the law "On The State Inspector Service" which entered into the force on May 10th 2019.

lighted that "Inspector is authorized to enter into restricted areas of the agency and monitor execution of activities by competent authorities in real time..., to obtain information about technical infrastructure used for the purpose of covert investigative measures and to inspect this infrastructure."[58] It is noteworthy, that according to the explanation made by the inspector at the court session, inspector had already been granted with this power; however, it was set in their order and not in the law.[59]

According to the public information requested from the Personal Data Protection Inspector's Office[60] within the scope of this research, "in 2017-2018 02 (two) unscheduled inspections of LEPL - Operative-Technical Agency of Georgia were made in order to study lawfulness of data processing as a result of covert investigative measures."[61] In the response from Inspector's office it is noted that, the inspection also covered the examination of the technical infrastructure intended for carrying out covert investigative measure under the sub-paragraph "b" of the first part of Article 143^1 of CPCG. Additionally, in 2016 the technical infrastructure for carrying out covert investigative action under the sub-paragraph "b" of the first part of Article 143^1 was also inspected within the scope of inspection of Operative-Technical Department of State Security Service of Georgia.[62]

Based on the above, it is obvious that the Personal Data Protection Inspector (according to the legislation being in force before May 10, 2019) and the successor in title of the Personal Data Protection Inspector – State Inspector Service has been carrying out inspection of technical infrastructure since 2016. This power was clearly established with the amendments to the Law of Georgia on "Personal Data Protection" on March 2017 (As a result of subsequent amendments made into the legislation, which entered into the force starting from May 10th 2019, the same rights are currently established in paragraph 7 of article 18 of the law "On The State Inspector Service"). However, as the personal data protection inspector[63] confirmed in the Constitutional Court, the inspector had been already empowered with this ability by the order. Under the circumstances, it is doubtful whether the function of inspection has actually undergone substantial changes, upon which the inspector had been granted with the power not available before. Finally, it should be noted that since the Constitutional Court has decided hearing on the merits of provisions related to obtain real-time internet communications, within the scope of existing disputes, it will be decided whether the functions defined by paragraph 7 of article 18 of the law "On The State Inspector Service" are sufficient to meet the requirement for "full and comprehensive inspection of technical infrastructure" mentioned in the judgment of April 14, 2016.

---

58 Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia, 58, 65-66.

59 Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia, 58-59.

60 According to the legislation being in force when requesting public information, "Personal Data Protection Inspector's Office" was still in force instead of "The State Inspector Service".

61 Response (№ PDP 7 19 00000216) from the Person Responsible for the Public Information of the Personal Data Protection Inspector's Office, January 21th, 2019 (in Georgian).

62 Ibid.

63 During the aforementioned constitutional dispute, the position of personal data protection inspector had been provided into the legislation.

5. Certain Problematic Aspects and International Practice

In the recording notice of Constitutional court of December 29, 2017, it is mentioned that obtaining information through the internet with stationary technical capability is not taking place since this is a costly system and at the same time it is less effective. The inefficacy of the system is due to transmission of information in encrypted form on the internet.[64] Additionally, according to the judgment of April 14, 2016 it has been confirmed that "so-called infecting technique" is used in practice for the purpose of real-time surveillance of internet communications. In legal terms, according to the applicable law, we can presumably consider "so-called infecting technique" under the "non-stationary technical capability" of obtaining real time communication, since according to the Law of Georgia "On Legal Entity of Public Law - Operative Technical Agency of Georgia", non-stationary technical capability is defined as data interception "during communication or after finishing communication without connecting to company's network or/and station infrastructure of electronic communication through special technical or/and software tools."[65] As for the semi-stationary technical capability, information on efficiency and usability in practice of this method is not available.

It is notable, that the Constitutional Court's judgment of April 14, 2016 does not define the meaning behind "so called infecting technique", discussion related to this technical capability is not developed in the judgment. As it has been already mentioned above, hacking (which also includes "so called infecting technique"[66]), as well as its technical capabilities is actively discussed in documents at international level, in human rights organization reports or foreign scientific literature and is under considerable attention, which is due to invasive nature of hacking and unlimited potential for access to broad range of information. As it is known, different types of information may be obtained after secret infiltration of computer system, therefore, different functionalities of hacking are available.[67] Taking into consideration the above mentioned, it is not clear what kind of surveillance measure is meant by judgment of the Constitutional Court in relation with "so-called infecting technique".

---

64 Different opinions of *Irina Imerlishvili, Giorgi Kverenchkhiladze and Maia Kopaleishvili* – Members of the Constitutional Court on Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia, 131.

65 The Law of Georgia on "Legal Entity of Public Law - Operative-Technical Agency of Georgia", subparagraph "G" of Article 2, <www.matsne.gov.ge>, [02.04.2019].

66 BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07.

67 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 58-59, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019]. See also *Sagers G.,* The Role of Security in Wireless Privacy, Compiled: Privacy in the Digital Age, 21st-Century Challenges to the Fourth Amendment, *Lind N.S., Rankin E.* (ed.), Vol. 2, California, 2015, 508. Access Now, A Human Rights Response to Government Hacking, 2016, 11, <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>, [03.04.2019].

Generally, in regards with hacking, it should be noted that because in modern internet network the communication is mostly encrypted, hacking may be one of the most effective method, and sometimes the only mean for investigation purposes. Meanwhile, its highly intrusive nature should be taken into consideration. Some European states specifically regulate the possibility of its use in the legislation, however as a rule, stricter approach and important guarantees of protection of rights are provided in this case.[68] One of the main objectives of criticism related to "hacking" is its application in the absence of specific legislative regulations.[69] The implementation of this measure may be only allowed if "explicitly prescribed by law", also if strict necessity and adequate guarantees are in place.[70] The requirement for "explicit regulatory framework" also implies that this method shall be regulated by the provisions, taking into account "unique privacy and security implications of hacking".[71] Legal provisions designed for conventional forms of secret surveillance, for example, telephone wiretapping, are not sufficient to provide adequate guarantees for hacking. Similarly, regulatory framework of "hacking", which repeats the rules of other electronic surveillance measures lack appropriate protection guarantees.[72]

As discussed above, secret surveillance measures need to be regulated by clear, transparent legal provisions according to "foreseeability" requirement. Clear and detailed provisions are necessary to ensure legality and proportionality in the context of electronic surveillance.[73] Depending on secret nature and invasiveness of these investigative measures, clarity of law is especially important in this context.

It should be underlined that sub-paragraph "b" of the first part of article 143[1] of CPCG regulating the investigative measures of internet surveillance, is so general that it covers obtaining communication through any means possible. This provision had been defined in the law of Georgia "On operative-investigative activities" prior to defining it in the CPCG as secret investigative action. As a result

---

68 BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07; *Vaciago G., Ramalho D. S.,* Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, 13, 2016, 92, 94-95, <http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252>, [03.04.2019]. See also *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 51-54, 58-61, 79-80, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

69 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 67, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

70 Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 18, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>, [03.04.2019].

71 Ibid.

72 Ibid.

73 Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 14-15, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement>, [02.04.2019].

of the amendments made in 2014, it was transferred to the Procedural Code unchanged. As the technology is developing rapidly, it is especially important that legislation keeps up with the pace. Because diverse and functionally different opportunities to access information resources are available, it is obvious that mentioned provision does not meet the requirement of legal clarity. According to the judgment of the Constitutional Court of April 14, 2016 sub-paragraph "b" of the first part of article 143^1 of CPCG implies "removal and recording of information from any communications channel, computer network and computer system, which consequently means monitoring of internet communications as well as access to information stored/generated in computer systems."[74] These two capabilities outlined by the court are absolutely different measures in content.

Taking into account international sources and the experience of European countries, clarity of regulations on obtaining internet communication is also underlined in regard with "so-called infecting technique", in particular, in the case when it's necessary to use different functionalities of hacking, it's recommended to separate basic functionalities at legislative level and to be the subject to a separate court authorization,[75] which is due to the fact that the influence on the right to privacy and the nature of the interference differs between various types of hacking, requiring different assessment of compliance with the principle of "proportionality".[76] This is also necessary to prevent overuse of extensive capabilities of hacking tool.[77] Such legislative differentiation of measures of obtaining information from computer systems is provided by, for example, the German Code of Criminal Procedure, where so-called "online search" and "telecommunications surveillance" (i.e. Source-TKÜ) are established in form of independent measures. "Online search" implies the interference with an information technology system with technical means, so data can be collected from the system without the knowledge of the person concerned. Under telecommunications surveillance monitoring and recording of real-time telecommunications may be carried out by intervening in an information system with technical means, without the knowledge of the person concerned.[78] This measure makes it possible to detect communi-

---

74 Judgment №1/1/625, 640 of April 14th, 2016 of the Constitutional Court of Georgia, 38.

75 *Gutheil M., Liger Q., Heetman A., Eager J. (Optimity Advisors)*, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 51, 89, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

76 Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 25, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>, [03.04.2019]. The document discusses the separation of authorization procedure for acquiring the information stored on computer system and real-time surveillance measures.

77 *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, 2017, 12, 58, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

78 Strafprozeßordnung (StPO), §100a Abs.1 S.2, §100b, <https://www.gesetze-im-internet.de-/stpo/index.html>, [03.04.2019]. The separation of main functionalities of "hacking" was also required under the judgement of Cassation Court of Italy, on July 1st, 2016. Regarding this Issue, see: *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identi-

cation before it is encrypted or after it has been decrypted.[79] In order to conduct these investigative actions in accordance with the legislative requirements, the software intended for the use can be applied only after passing the relevant testing and conforming to the minimum standards established specifically.[80] This mechanism is an important guarantee against excessive, illegal use of technical capabilities related to these investigative measures.

Taking all these into consideration, it is recommended that the types of electronic surveillance under sub-paragraph "b" of the first part of article 143^1 of CPCG be clearly defined in order to differentiate the rights to obtain real-time communications and access to information stored on computer system.

Parallel to providing legal clarity in sub-paragraph "b" of the first part of article 143^1 of CPCG, it is also important that the judge should be informed about the specific technical means intended for requested surveillance measure in every individual case. While evaluating the proportionality of secret investigative action, one of the most significant measurement is the potential of the technical tools used with regards to interfering with the right to privacy. The proportionality of the measure restricting the right to privacy and allowing the possibility of electronic surveillance by using specific technical devices depends on the knowledge of relevant bodies about the scope of the measure and applicable technical tools. This implies that the interference with privacy caused by specific covert investigative measure should be assessed in advance.[81] In this context it should be taken into account that according to CPCG, neither in Prosecutor's motion nor in court ruling on authorizing the secret investigative action, information on technical means is not determined as mandatory requisite, according to which specific measure shall be carried out.[82] Providing the information about the technical means used is only required in the protocol of covert investigative activity, however this document is only drawn up only after the end of executed measure.[83] As for court ruling or prosecutor's motion, data defined as mandatory requisites for these documents by the CPCG is not sufficient for the judge to have a sufficient understanding how the investigative measure is going to be implemented in practice. Consequently, it seems difficult to properly assess if the proposed measure is in fact least intrusive, necessary and proportional mean for privacy interference.

---

fication, Evaluation and Comparison of Practices, 2017, 85, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>, [03.04.2019].

79 <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html>, [03.04.2019].

80 <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html>, [03.04.2019].

81 *Milaj J.,* Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol.30, No 3, 2016, 115.

82 See CPCG, part 10 of article 143^3.

83 See CPCG, part 14 of article 143^6.

6. Conclusion

Thus, in the present paper, certain problematic aspects related to monitoring the internet communications have been reviewed. Sub-paragraph "b" of the first part of article 143^1 of CPCG was underlined as unclear and formulated imprecisely, which enables the usage of all available methods for internet surveillance under this provision. In the modern age the methods of obtaining private information through electronic means for investigation purposes are diverse, and respectively, possible impact on the right to privacy and the degree of intrusion in many cases is not the same, which may require different assessment of the proportionality test in a certain case. Accordingly, precise regulatory framework in regard with online surveillance is essential. As an illustration, an example has been provided on the German legislation, where the "online search" of computer system and the "telecommunication surveillance" are established as independent surveillance measures. In addition to the aforementioned, for comprehensive analysis of the aspects related to proportionality requirement in an individual case, it is necessary that prosecutor's motion and court ruling shall clearly define precise information on the ways of conducting secret investigative actions: technical means intended to interfere with the right to privacy.

Considerable attention has also been paid to the judgement of the Constitutional Court of Georgia of 14 April, 2016 in relation to usage "so-called infecting technique" in practice. From this point of view, it is not clear what kind of technical capability is meant by this term. The judgment did not focus on the specific content and invasiveness of this measure. As it has already been mentioned, there are various types of this measure. Some European countries specifically regulate the application of certain functionalities of hacking and relevant guarantees in the legislation. It is considered that provisions related to other surveillance measures, for example telephone wiretapping, are not sufficient in this regard and a stricter approach should be developed due to the intrusiveness of hacking tool. Therefore, if using of "so-called infecting technique" is necessary in practice of Georgian law enforcement agencies, precise legal framework, different, stricter approach and adequate guarantees should be in place.

Bibliography:

1. Constitution of Georgia, Departments of the Parliament of Georgia, 31-33, 24/08/1995.
2. Criminal Procedure Code of Georgia, LHG, 31, 09/10/2009.
3. Law of "LEPL Operative-technical Agency of Georgia", 22/03/2017.
4. Strafprozeßordnung (StPO) Deutschlands, 07/04/1987.
5. CCPR General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), UN Human Rights Committee, 08/04/1988.
6. CCPR General Comment No. 27: Article 12 (Freedom of Movement), UN Human Rights Committee, 02/11/1999.
7. Comment to the Constitution of Georgia, Chapter Two, Citizenship of Georgia, Human Rights and Freedoms, Tbilisi, 2013, 181 (in Georgian).

8. *Corn G. S., Brenner-Beck D.,* "Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance", The Cambridge Handbook of Surveillance Law, *Gray D., Henderson S. E.* (ed.), New York, 2017, 334-335.
9. *Clough J.,* Principles of Cybercrime, New York, 2010, 135, 136, 153-154.
10. *Haase A., Peters E.,* Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance, International Data Privacy Law, Vol. 7, No. 2, 2017, 126, 130-131.
11. *Kerr O. S.,* The Next Generation Communications Privacy Act, University of Pennsylvania Law Review, Vol. 162, No. 2, 2014, 384.
12. *Loideain N.,* EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communication, Vol. 3, No 2, 2015, 54.
13. *Milaj J.,* Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance, International Review of Law, Computers & Technology, Vol. 30, No. 3, 2016, 115.
14. Response (№ PDP 7 19 00000216) from the Person Responsible for the Public Information of the Personal Data Protection Inspector's Office, January 21th, 2019 (in Georgian).
15. *Sagers G.,* The Role of Security in Wireless Privacy, in the book: Privacy in the Digital Age, 21st-Century Challenges to the Fourth Amendment, *Lind N. S., Rankin E.* (ed.), Vol. 2, California, 2015, 508.
16. *Swire P.,* From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek access to the Cloud, International Data Privacy Law, Vol. 2, No. 4, 2012, 202-203.
17. *Vaciago G., Ramalho D. S.,* Online Searches and Online Surveillance: The Use of Trojans and other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings, Digital Evidence and Electronic Signature Law Review, Vol. 13, 2016, 88-89, 92, 94-95, <http://journals.sas.ac-.uk/deeslr/article/viewFile/2299/2252>.
18. *Winter L. B.,* Remote Computer Searches under Spanish Law: The Proportionality Principle and the Protection of Privacy, Zeitschrift für die Gesamte Strafrechtswissenschaft, Vol. 129, No. 1, 2017, 211-212.
19. *Wright J.,* Necessary and Inherent Limits to Internet Surveillance, Internet Policy Review, Vol. 2, No. 3, 2013, 1.
20. Access Now, A Human Rights Response to Government Hacking, 2016, 11, <https://www.accessnow.-org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>.
21. Encryption and Anonymity Follow-up Report, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2018, 7, 18, <https://www.ohchr.org/Documents/-Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>.
22. *Gutheil M., Liger Q., Heetman A., Eager J.* (*Optimity Advisors*), Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (Study for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs), Policy Department for Citizens' Rights and Constitutional Affairs, 2017, 12, 42-43, 51-54, 58-61, 67, 79-80, 85, 89, <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf>.
23. International Principles on the Application of Human Rights to Communications Surveillance, <https://en.necessaryandproportionate.org/text>.

24. Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, Privacy International, 2018, 8, 18, 25, <https://privacyinternational.org/sites/default/files/201808/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>.
25. Report of the Office of the United Nations High Commissioner for Human Rights, The right to Privacy in the Digital Age, 30.06.2014, 9, <https://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc>.
26. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23.09.2014, 14-15, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement>.
27. Report of the Special Rapporteur "On the Promotion and Protection of the Right to Freedom of Opinion and Expression", 17.04.2013, 4, 10, 11, 18, <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>.
28. Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia, 58, 59, 65-66.
29. Dissenting Opinion of the Members of the Constitutional Court of Georgia – Irine Imerlishvili, Giorgi Kverenchkhiladze, Maia Kopaleishvili to the Recording Notice of Recording Notice №3/4/885-1231 of December 29th, 2017 of the Constitutional Court of Georgia, 131.
30. Judgment №1/1/625, 640 of April 14th, 2016 of the Constitutional Court of Georgia, 28, 38, 54, 55-56, 57-58.
31. Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB and Watson, [2016], Court of Justice, 98-100.
32. Szabo and Vissy v. Hungary, [2016] ECtHR, 73.
33. Roman Zakharov v. Russia, [2015] ECtHR, 227, 229, 230, 232.
34. Case NC-293/12 and C-594/12, Digital Rights Ireland ltd and Seitlinger and others, [2014], Court of Justice, 34.
35. Kennedy v. United Kingdom, [2010] ECtHR, 130,153.
36. BVerfG, Judgment of the First Senate of 27th February 2008 - 1 BvR 370/07.
37. Association for European Integration and Human Rights and Ekimdzhiev, [2007], ECtHR, 75.
38. Weber and Saravia v. Germany, [2006], ECtHR, ECHR 2006-XI, 106.
39. Valenzuela Contreras v. Spain, [1998], ECtHR, Reports 1998-V, 46.
40. Huvig v. France, [1990], ECtHR, (Ser. A.), 32.
41. Kruslin v. France, [1990], ECtHR, (Ser. A.), 33.
42. Leander v. Sweden, [1987] ECtHR, (Ser. A.), 51.
43. Malone v. United Kingdom, [1984], ECtHR (Ser. A.), 67.
44. Klass and others v. Germany, [1978] ECtHR, 1978, (Ser. A.), 49-50, <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung.html>.