Goga Khatiashvili

HOW THE LEGISLATION AND PRACTICE ON REQUESTING INFORMATION FROM THE COMPUTER SYSTEM HAS DEVELOPED

Goga Khatiashvili
LL.M, Ivane Javakhishvili Tbilisi State University.

ABSTRACT

Requesting information from the computer system was a subject to discussion for a long period. Initially, only the prosecution side had the exclusive competence to conduct this investigative activity, which was viewed as breach of the principles of adversarial process and equality. Along with the legislation, inconsistent judicial practice created even more obstacles for the defense to obtain information from computer system (video recordings, information store in computer and mobile equipment, etc.). The mentioned challenges were partially addressed by the Constitutional Court in its decision of 27 January of 2017, however, number of legislative and practical gaps still remain, which creates difficulties for the parties in the process to obtain such evidence.

The article tries to discuss the legislation and practical approaches regarding retrieving information from computer system. For this reason, in the article there will be presented the analysis of the legislation and practice existing before the judgement of the Constitutional Court, as well as interpretations established after that judgement. Therefore, readers will have possibility to follow the tendency, which undergoes significant changes in recent couple of years and see clearly the role of the decision of Constitutional Court in enhancement of the circle of subjects who have title to conduct this investigative activity.

INTRODUCTION

In the criminal legal proceedings, it becomes more important to retrieve evidence from such channels, which exist in electronic form. Public institutions as well as private organizations/individuals widely use digital technologies, which afterwards become subject of interest for investigation. Electronic communication is important not only for establishing personal relationships, but also in terms of business communications. On the one hand, it is possible that the computer is a tool for committing crime, but on the other hand, computer system/electronic equipment stores evidence incriminating the conduct of crime. In the latter case, it is important that parties have equal and proper possibility to retrieve the data stored in computer system and present it before a court as an evidence.

The current article aims to evaluate legislation and subsequent practice on requesting information from computer data, which in recent years undergoes significant changes. For this purpose, analyses of relevant case-law of common courts will be presented considering the practice existing before the judgement of the Constitutional Court, as well as in light of tendencies developed after this judgement. Despite certain positive and well-grounded court decisions, there is still a problem not only in terms of unequal possibilities for retrieving this information, but also difficulties related to obtaining of such evidence.

1. ANALYSIS OF THE LEGISLATION

Because of the wide usage of scientific-technical progress and computer technologies in the criminal legal proceedings, the necessity emerged to regulate the rules for treating the data stored in computer system. For this purpose, from September 30, 2010, requesting documents or information, which is stored in the computer system or mean for storing the computer data appeared in the Criminal Proceedings as a separate investigative activity and the entitlement to implement this activity was given only to the prosecution. Also, legislation defined the computer system, computer data and respective definitions were introduced to the Code of Criminal Proceedings (hereinafter: CPC) in paragraphs 27 and 28 of Article 3. According to these definitions, computer system is any mechanism or group of inter-related mechanisms, which automatically process the data through the program. This mechanism may be personal computer, mobile phone and any other tool. As for the computer data, the law defines it as information/program expressed in any form accessible for processing in the computer system, and it ensures functioning of the computer system.

Procedures for carrying out this investigative activity were amended in August 2014 and requesting documents or information became possible only with the same rules and standard applicable to the secret investigative activities. Carrying out secret investigative activity is impossible on every category of crime. In particular, the secret investigative activity may be conducted only in case the investigation is initiated and/or prosecution is carried out for intentional serious and/or particularly serious crime. Moreover, on some of the less serious crimes, the comprehensive list of which is presented in the paragraph 2 subparagraph "a" of the Article 143[3] of CPC. This limitation is spread to the requesting information from the computer system. Therefore, for the prosecution side several restrictions were introduced, which entailed obliging investigative bodies to lead the secret investigative activities with respective standard. Hence, requesting information from computer data represents a special case of seizure, which exists as independent investigative activity[1] and is carried out according to the rules characteristic to secret investigative activities.

Initially, the possibility to carry out such investigative activities was given only to prosecution and the law did not let the defense to retrieve information stored in the computer system. Therefore, as it is defined in literature, if the defense side had the information that important data for the ongoing case was stored in the computer system, it should have filed a motion for the prosecutor, who on his/her own would address the judge with the motion on the request of this information.[2] Hence, the defense could obtain information stored in the computer system or computer data storing tool only through the prosecutor.

The fact that the defense had no right to obtain information stored in the computer system was assessed negatively by several lawyers and scholars. Such unequal approach with regard to the parties to the process was considered unjustified and substantial infringement of the principle of adversarial process.[3]

2. INTERPRETATIONS AND TENDENCIES ESTABLISHED IN THE COURT

In a well-established case-law of common courts, obtaining information from the computer data was interpreted widely. The majority of judges considers that any information stored in the

1 Commentaries to the Criminal Procedure Code of Georgia, edited by G. Giorgadze, of 1 October 2015, printing house "Meridiani", Tbilisi, 2015, 422.

2 Commentaries to the Criminal Procedure Code of Georgia, edited by G. Giorgadze, of 1 October 2015, printing house "Meridiani", Tbilisi, 2015, 423.

3 Democratic Initiative of Georgia, Report on the implementation of the I and II chapters of the Action plan, 13-14, http://bit.ly/2zLNmvH [20.03.2019]; Also see: Evidence in the criminal law process, Tbilisi, 2016, 153-154, http://bit.ly/2zCw7Q4 [20.03.2019]; Also see: Obtaining evidence by the defense side through the court, research and recommendations, Association of Law firms of Georgia, Tbilisi, 2015, 33,35.

computer system represents an object protected under the Article 136 of the CPC. Therefore, it was defined that Article 136 of the CPC is a special (exceptional) norm, which regulates the method of obtaining information stored in the computer system or tool for storage of computer data, and for that, instead of "seizure", "request" shall be carried out by relevant law enforcement agencies.[4] The different reasoning is presented by the judge of the Tbilisi Appellate Court in the ruling of 2015. In the opinion of the judge, Articles 136-138 of CPC stipulate procedural rules for investigating such crimes that may be committed by using computer system and not any information, which may be stored in the computer system/tool. Hence, according to the judge, mentioned provisions are only related to investigation of crimes committed through computer system, where the computer system was used. However, mentioned ruling had not a nature of tendency and neither had respective application in the practice.[5]

The Courts impose strict and high standards on requesting of information from computer system due to protect privacy and personal data.[6] In the view of the judges of investigative collegium of the Tbilisi Appellate Court, when there is an occasion of requesting information stored in the computer system by the investigating body, this activity shall be carried out in a manner as secret investigative activity and not ordinary investigative activity. Moreover, the court established that voluntariness does not cover the secret investigative activities, as far as this activity would lose the criminal law meaning that is needed for retrieving information in secret regime.[7] Consequently, courts put emphasis on the nature of evidence and indicate that in the information stored in the computer system shall be obtained by the investigation in any case based on the Articles 136 and 143^{2}-143^{10} of the CPC.

However, at the same time, the judges indicate that in cases when investigation is initiated for the fact of less serious crime, investigative bodies shall obtain information on the basis of Articles 125-126 of the CPC and conduct inspection. Hence, the court considers that if the category of crime does not let defense to obtain information from computer system, then the inspection shall be carried out and in such a way, the information necessary for the case shall be obtained. In addition, the court interprets that this procedure must not become similar to the request of information.[8] On one of the cases, the Appellate Court rejected the motion of prosecutor with the motive that the procedural requirement were not sustained during the obtaining of video recordings. In particular, the ground for transmitting video recording on the CD by the private individual to the investigation was the application of the investigator and not a court ruling (or ordinance of the prosecutor in urgent necessity). The Appellate Court defined that it is inadmissible to request the information prescribed under the Article 136 of the CPC based on the application for the side of investigator.[9]

4 Ruling of the Tbilisi Appellate Court, N1g/960-17, 19 July, 2017.

5 Obtaining evidence by the defense side through the court, research and recommendations, Association of Law firms of Georgia, Tbilisi, 2015, 25-27.

6 Ruling of the Tbilisi Appellate Court, N1g/1537-16, 4 October 2016.

7 Rulings of the Tbilisi Appellate Court: №1g/118, 5 February 2015; №1g/119, 7 February 2015; №1g/548, 30 March 2016.

8 Ruling of the Tbilisi Appellate Court, N1g/1537-16, 4 October 2016.

9 Ruling of the Tbilisi Appellate Court, N1g/337-17, 9 March 2017.

Therefore, according to the practice established in common courts, for receiving information stored in computer system the court required from the prosecution to follow certain criteria:

- Prosecutor must ask for the request of information from computer data and not "seizure";
- Prosecutor shall obey the regime defined for the secret investigative activities, and also consider the category of the crime;
- In the motion, prosecution must indicate as a legal basis the respective norms: Articles 136, 143^{2}-143^{10} of the CPC.

Hence, the judge calls upon the prosecution to pay attention to the type of information and procedural rules for its obtaining when initiating a motion.[10]

As for the motion of the defense, the court explained that according to the legislation defense did not have possibility to file a motion on the request of information from computer system, as far as the law gave such competence only to prosecutor.[11] Thereby, in case if the defense asked for seizure of the information stored in the computer system, as a rule, such motion was not admissible and the judge indicated that obtaining information from the tools storing the computer data must be carried out through requesting. In addition, judges defined that the author of the motion for such an investigative activity (requesting) may not be the defense.[12] Though, courts gave right to the defense to conduct inspection if the motion was properly justified.[13] Consequently, in most cases, the defense had access to the information store in the computer system, only by means of inspection. In light of the established restriction on one hand, and wide definition of computer system in practice on other hand, defense had possibility to receive information in material form (for instance recording on CD) and in certain cases only exercise the right for inspection.

It should be noted that although video recordings are considered as data stored in computer system, there were exceptions when the court did not consider the video recordings filmed by the badge video eye of patrol police and vehicle video registrar as information stored in computer system. Therefore, the court entitled the defense to conduct seizure.[14]

10 Ruling of the Tbilisi Appellate Court, N1g/1497, 20 September 2016.

11 Ruling of the Tbilisi Appellate Court, N1g/1430, 6 September 2016.

12 Obtaining evidence by the defense side through the court, research and recommendations, Association of Law firms of Georgia, Tbilisi, 2015, 23.

13 Obtaining evidence by the defense side through the court, research and recommendations, Association of Law firms of Georgia, Tbilisi, 2015, 21-24.

14 Obtaining evidence by the defense side through the court, research and recommendations, Association of Law firms of Georgia, Tbilisi, 2015, 23-24.

2.1. Inspection of the information stored in the computer system

According to the Article 125 of the CPC, for the purpose of finding out trace of crime, discovering physical evidence, finding out other conditions relevant for the criminal law case, a party has right to inspect the place of incident, storage, dwelling place, storeroom, human corpse, item, document or other object containing information. Inspection may be conducted by using three different regimes: by prior permission from the court, in the circumstance of urgent necessity or on the basis of a written consent of owner (possessor).

The Courts had made an interesting interpretations with regard to the obtaining of information relevant for the case during the inspection. In particular, during the inspection, a person conducting this investigative activity has the right to seize the item, document, substance or any other object containing information after the inspection. However, such reservation does not relate to cases, which are connected to computer system or inspecting tool for storing computer data. Hence, when a judge issues permission for inspection, automatically this permission spreads over the seizure, taking place during inspection, but investigative collegium explains that similar permission may not be spread on the seizure of information existing in the form of computer data. Judges call upon prosecution that in case the scheduled inspection may in perspective involve necessity to obtain computer data the prosecutor must file a motion with the court on inspection, as well as on requesting the information.[15]

Also, the Courts made interesting interpretations with regard to the inspection of the information obtained unlawfully. In the case concerned, the witness introduced to the investigation the video recording voluntarily. The prosecutor addressed the court with the motion on requesting permission to inspect the information "given voluntarily". A Judge from the investigative collegium stated that the information for inspection of which the prosecutor requested permission was not obtained in accordance of procedural provisions. Therefore, Investigation obtained this information from the voluntary introduction from the witness and attached to the case with the inspection report, however the court indicates, that voluntary introduction of the DVD disk was not a lawful way for its obtaining and it was necessary from the side of investigation to follow the rules established for the request of information from computer data. Hence, the judge makes a conclusion that issuing permission by the court for inspecting such information which is obtained by significant infringement of law, opposes to the principle of legality and the court is not entitled to approve the query for issuing a ruling for inspection of those evidence that were obtained through the significant breach of the law.[16]

15 Ruling of the Tbilisi Appellate Court, N1g/1497, 20 September 2016.

16 Ruling of the Tbilisi Appellate Court, N1g/109, 25 January 2017.

2.2. Voluntary transmission of information stored in the computer system

In practice, the issue of voluntarily transmit of the information stored in the computer system to the investigative bodies was out high on the agenda. As the courts define, in comparison to the Criminal Procedure Code from 1961, voluntary introduction as an investigative or procedural activity does not exist. Therefore, existing legislation does not recognize the investigative activity titled as "voluntary introduction". The judge points out that if the transfer of the object containing information is carried out voluntarily, an investigator must file a report on particular investigative activity or considering specifics of the investigative activity – must be out under the court control.[17] In the court ruling of 16 February 2017 N1/552-17 it is stated – instead of obtaining the court ruling for requesting information stored in the mobile phone, the defense directly applied to the owner and obtained the recording in a way which infringes requirements of the Article 136 of the CPC. The rules envisaged for the secret investigative activity factually excludes possibility to conduct investigative activity in conditions of one-sided communication, because of what in all cases, deriving from the question specifics, the high standard and possibility of judicial control shall be preserved.

3. ANALYSIS OF THE DECISION OF CONSTITUTIONAL COURT FROM 27 JANUARY 2017

The Constitutional Court has deliberated on the constitutionality of the Article 136 of the CPC, and assessed the constitutionality of the impugned provision with regard to the paragraph 3 of the Article 40 and paragraph 1 and 3 of the Article 42 of the Constitution.

According to the definition of the Constitutional Court, impugned provision does not directly point to the restriction on filing motion by the defense, however, as the special subjects for filing such motion are comprehensively defined in the law, the will of the legislator in relation to granting such authority only to the prosecution.[18] In addition, the court concludes that such regulation creates procedural reality where the defense does not have possibility to confront with the prosecution, present justified counterarguments and justifiable evidence on the prosecutions side. Hereby, the judges consider that obtaining computer evidence by the defense entirely is related to the "good will" of the prosecution.[19] It is unclear for the court what is the legitimate aim of restricting the possibility of the defense to file a motion before the court and obtain the justifiable evidence,

17 Ruling of the Tbilisi Appellate Court, N1g/109, 25 January 2017.

18 Decision of the Constitutional Code of Georgia "Citizens of Georgia Natia Khurtsidze and Dimitri Lomidze v. Parliament of Georgia", 27 January 2017, N1/1/650,699,12.

19 Decision of the Constitutional Code of Georgia "Citizens of Georgia Natia Khurtsidze and Dimitri Lomidze v. Parliament of Georgia", 27 January 2017, N1/1/650, 699, 20.

when the legislation give the defense right to search and seize, which in certain cases may create threat to interfere in the private life and personal sphere of third persons with higher intensity.[20]

Therefore, the court assesses as unconstitutional the normative content of the regulation which restricts the right of defense to obtain, independently from the prosecutor, information stored in the computer system.

4. HOW THE JUDICIAL PRACTICE DEVELOPED AFTER THE JUDGEMENT OF THE CONSTITUTIONAL COURT?

After the decision of the Constitutional Court, the common courts started to examine requests on obtaining the computer data for the defense, although, subsequent practice developed extraordinarily. Initially, it is important to emphasize the practice of interpreting constitutional court decisions by the judges of common courts. Mainly, the approaches of judges are homogenous, however there are exceptions too, which were not implemented or used widely in practice. Mostly, the approach of judges is based on proper analysis of the constitutional court decision and they indicate that constitutional court have discussed only in the context of subjects[21] entitled to file a motion at court with regard to conduct of investigative activity - requesting information and the Constitutional Court did not declare unconstitutional the first and third paragraphs entirely of the Article 136 of the CPC. According to the definition of the court, only the normative content of the impugned provision was considered as unconstitutional, and other normative contents, including introducing restrictions for prosecutor still remained constitutional.[22] Besides, extremely controversial interpretations of the constitutional court were stated. In one of the rulings of the Tbilisi City Court which was reflected in later ruling of the appellate court, it is indicated that the defense is entitled to file a motion on requesting to conduct investigative activities envisaged in the Article 136 of the CPC, however at the same time, the court explains, that, as far as for the request of information is covered by the secret investigative activity procedures, the defense does not have the right to request such information.[23] Hence, the court has admitted the right of the defense to obtain the information stored in computer data, but, in fact, refused the realization of this right.

20 Decision of the Constitutional Code of Georgia "Citizens of Georgia Natia Khurtsidze and Dimitri Lomidze v. Parliament of Georgia", 27 January 2017, N1/1/650, 699, 22.

21 Ruling of the Tbilisi Appellate Court, N1g/263-17, 22 February, 2017.

22 Ruling of the Kutaisi Appellate Court, N1g/289, 16 June, 2017.

23 Ruling of the Tbilisi Appellate Court, N1g/334-17, 7 March, 2017.

The investigative collegium of Appellate Court did not agree with this reasoning of the first instance court and approved the claim of the defense on the granting permission for conducting request. There is one more interesting ruling which also was not the basis for changing primarily established tendency in the courts. By virtue of this decision, the judge from the investigative collegium of the appellate court explained that declaring unconstitutional certain normative content of the norm is equivalent of declaring the norm itself as unconstitutional, therefore, in the view of the judge, paragraphs 1 and 4 of the Article 136 of the CPC were declared unconstitutional and void entirely. Moreover, the investigative collegium states that by virtue of the judgement of the Constitutional Court this investigative activity returned to its own margin as far as the existing procedure for requesting information and documents never represented the secret investigative activity, hence it was not correct to spread the application of the regulations on secret investigative actions on this investigative action.

> "It is true that request of information and documents may restrict the private property, possession or inviolability of personal privacy, but not in such extent and standard, as it is during the secret investigative activities."

In light of the given reasoning, the judges established that requesting information stored in the computer system by its nature represents ordinary investigative activity and not the secret one. Therefore, while requesting such information, parties must not follow the reservation in paragraph 4 of the Article 136 of the CPC (as far as it does not exist anymore, it is void and unconstitutional) and norms of secret investigative activities.[24] Despite this exceptional approach, according to the mainstream opinion, the prosecution is still not entitled to retrieve the information stored in the computer system by omitting rule defined for the secret investigative activity.[25] In particular, for the crimes of less serious nature (not including exceptions) the prosecution was not and is not entitled to conduct secret investigative activity, including requesting information stored in the computer system.[26]

Therefore, after the judgement of the Constitutional Court, the prosecution still is guided by the same rules and the court still requires the prosecutor to fulfill the same criteria, as it was before the judgement. In this regard, approaches of the legislation and practice toward the prosecution, have not been significantly changed. In certain occasions, the restrictions toward prosecution to retrieve the information on all categories of crime are considered unjustified by the judges but they assess it as a gap of the legislation. In particular, in view of the judge, there shall be no obstacles for the investigation in retrieving evidence due to the gap in legislation, however, at the same time judge considers that the court is obliged to follow the requirements of the law. Therefore, as assessed by the judge, evaluating the adequacy of the law and searching for an outcome passing by the law or by virtue of improper interpretation does not fall within the competence of the court.[27] The judge

24 Ruling of the Tbilisi Appellate Court, N1g/757, 2 June, 2017.

25 Ruling of the Tbilisi Appellate Court, N1g/858-17, 21 June, 2017.

26 Ruling of the Tbilisi Appellate Court, N1g/552-17, 16 February, 2017.

27 Ruling of the Tbilisi Appellate Court, N1g/109, 25 January, 2017.

made such explanation in the context that the prosecution does not have possibility to request information stored in the computer system on the less serious crimes category (if there are no exceptions).

In many court rulings, the prosecution express dissatisfaction because of the fact that defense has a possibility to retrieve information from the computer system on all categories of crime, while the prosecutor is not entitled to do so. Hence, prosecutors indicate that nowadays, defense may request information according to general rules established for the investigative activities and apply to the court with motion on less serious crime as well.[28] It is interesting that there is no consistent practice and case-law with regard to obtaining information by the defense.

In particular, city/district court judges indicate that provision of secret investigative activities still apply to the requesting of information stored in the computer system with only distinction that defense also has the right to address the court on this matter. Moreover, the court considers that realization of this right given to defense must be implemented according to the general provision of the CPC.[29]

There is an interesting discussion in the rulings of Kutaisi City Court, in particular, the Court stated that standards established by the legislation to conduct secret investigative activities, which is related to the filing motion and discussing it in line with the principles of secret legal proceeding, cannot be applied to defense.[30] We may find different interpretations in one of the city court rulings, according to which, the defense has no authority with regard to the secret investigative activities, however, at the same time, it defines that deriving from the judgement of the Constitutional Court, defense is restricted in requesting such information with categories of crimes.[31]

The same approach is shared in the collegium of the Tbilisi Appellate Court. According to the interpretation of the Appellate Court, the judgement of the Constitutional Court and existing legislation does not put any of the parties in preferential position, therefore, there are restrictions and permissions set for both parties equally while requesting information stored in the computer system.[32]

Hence, based on the court interpretation, in case of the less serious crime category, neither defense nor prosecution has the right to file a motion on requesting such information.[33]

28 For instance, the prosecutor indicates about this in several appellate complaints, which later on are reflected in the appellate court rulings. See: Rulings of the Tbilisi Appellate Court: Ruling N1g/859-17 of 21 June 2017, Ruling N1g/975-17 of 20 July 2017, Ruling N1g/757 of 2 June 2017.

29 Rulings of Zugdidi District Court: 9 May 2017, 19 May 2017.

30 Ruling of the Kutaisi City Court: 28 March 2017, 18 May 2017.

31 Ruling of the Poti City Court of 29 March 2017.

32 Ruling of the Tbilisi Appellate Court, N1g/858-17, 21 June, 2017.

33 Ruling of the Tbilisi Appellate Court, N1g/975-17, 20 July, 2017.

In case the investigation is initiated for the fact of less serious crime, information must be obtained on the basis of Articles 125 and 126 of the CPC and the inspection must be conducted.[34] As it is indicated in the decision, based on the conduct of inspection it will be defined whether the crime was committed and/or the information imprinted there is relevant for important circumstances of the criminal case.[35] Therefore, according to the established case-law of common courts, despite the possibility of the defense to obtain an information stored in the computer system, he/she is obliged to pay attention to the crime qualification, which is characteristic to the secret investigative activities.

The Appellate Court additionally points out that the Constitutional Court along with granting the right to the defense to obtain information stored in the computer system, imposed an obligation to refrain from creating threat of interference in the private life and private property of third persons. The court indicates that this obligation of the defense will be measured by the level of justification of the motion.[36]

In addition, according to the court's ruling, the motion on retrieving the evidence must be based on the certain objective information, as far as without any justified ground it is prohibited to transfer the computer information. Hence, the court points to the defense that it must consider features of the video recording, existence of the information on the third person and in conditions of special justification retrieve such information. Thus, according to the court assessment, in the computer system there are plenty of personal data of individuals, however in case of firm justification, when this information has a value for the criminal case, it is possible to interfere in the private life or private property.[37] Consequently, the court mainly asks the defense to maintain the criteria mentioned below, which must be considered while presenting the motion:

- The motion must be presented within the scope of regulation prescribed by law (Article 136 of the CPC);
- In the motion, there must be indication/justification that the requested information really exists and is stored in the computer system. For instance, in case of requesting video cameras, the defense must provide information on whether there are CCTV situated in the respective area and recording;
- In particular cases, the judge points to the defense to request information from the body controlling CCTV/authorized person, whether the CCTV provides recording and fixing the data.[38]
- Requested information must be important for the defense and having the evidential significance for the case concerned.

34 Ruling of the Tbilisi Appellate Court, N1g/975-17, 20 July, 2017.

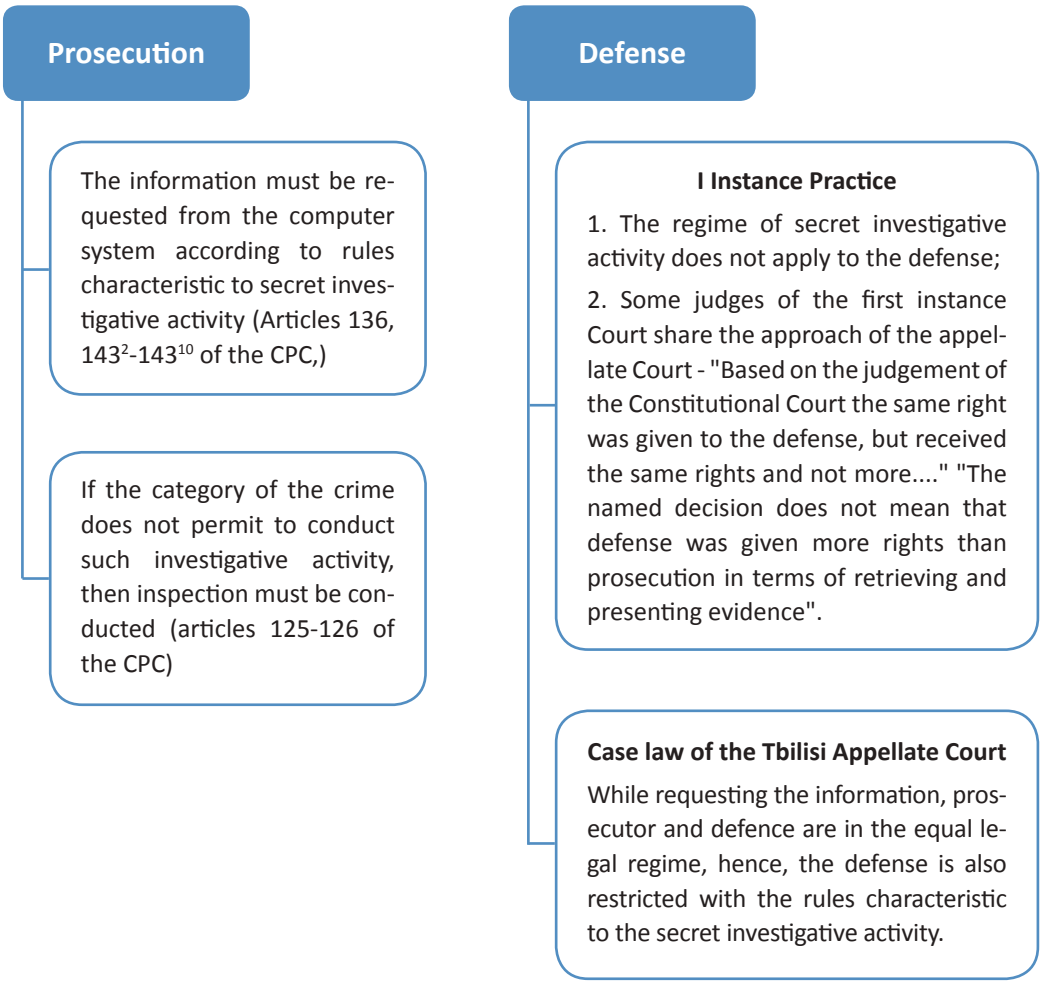
35 Ruling of the Tbilisi Appellate Court, N1g/858-17, 21 June, 2017.

36 Ruling of the Tbilisi Appellate Court, N1g/406-17, 21 March, 2017.

37 Ruling of the Tbilisi Appellate Court, N1g/536-17, 13 April, 2017.

38 Ruling of the Kutaisi City Court, N11/a-117, 18 May 2017.

The diagram below demonstrates approaches of courts with regard to requesting information stored in the computer system



CONCLUSION

In conclusion, existing legislation and subsequent practice developed by common courts, requires that information stored in the computer system must be retrieved in any case in line with the Articles 136 and 143²-143¹⁰ of the CPC. However, when the investigation is initiated on the fact of committing less serious crime, retrieving information related to the computer data is possible under the Articles 125-126 of the CPC by conducting inspection.

For the adversarial proceeding and equality, it is important that parties have equal/similar possibilities to obtain evidence. The principles of equality and adversarial proceedings are infringed when the legislation and practice put one party in a preferable situation and gives insufficient tools to the other party in relation to activities of similar nature.

Requesting information from the computer system does not involve personal data to such extent that the high standard of secret investigative activity shall be used and information shall be limited to the certain categories of crimes only. Moreover, information stored in the computer system is frequently needed while dealing with less serious crimes, therefore the parties shall not have significant obstacles to receive it.

In this regard, not only legitimate interests of investigation are damaged, but also the right of the defense to retrieve and present to the court the evidence proving the innocence of the defendant. Therefore, legislative amendments should be adopted to classify requesting information stored in the computer system as an independent investigative activity and must not take over the standard characteristic to the secret investigative activity. Such legislative regulations will give both parties an equal opportunity to retrieve information stored in the computer system in cases of all categories.