



Instituti i Kosovës për Drejtësi  
Kosovo Law Institute  
Kosovski Institut Pravde



# EXAMINATION OF PHONES WITHOUT COURT DECISION

18/25





Author: Gzim Shala

Contribution: Alberta Hashani

Editors: Ehat Miftaraj and Betim Musliu

No part of this material may be printed, copied, reproduced in any form, electronic or printed, or in any other form of reproduction without the permission of the Kosovo Law Institute.

Implemented by:



Instituti i Kosovës për Drejtësi  
Kosovo Law Institute  
Kosovski Institut Pravde

## ABOUT KLI

Kosovo Law Institute, is a non-profit organization of public policy, a think-tank specialized in the justice sector.

KLI, Str. Ilaz Agushi

Pristina

Email: [info@kli-ks.org](mailto:info@kli-ks.org)

[www.kli-ks.org](http://www.kli-ks.org)

December, 2025

Pristina, Republic of Kosova

## Contents

1.	Executive summary .....	5
2.	Background of the problem .....	6
3.	Court decision for examination of a phone.....	7
4.	Retroactive interceptions .....	8
5.	Are material found on a phone interceptions? .....	8
6.	Constitutional compatibility of the provisions .....	9
7.	Compatibility of the provisions with the jurisprudence of the EctHR.....	10
8.	Avoidance of applying a law in contravention of the Constitution .....	12
9.	Practical consequences .....	14
10.	Conclusions .....	14
11.	Recommendations .....	15

## 1. Executive summary

Recently, a public debate has emerged regarding which authority is competent to authorize the examination of seized mobile devices: whether a court order for seizure is sufficient, or whether a separate judicial decision is also required for examining the data contained in the device. This debate intensified in particular following a concrete case before the Basic Court in Pristina, where evidence obtained from the examination of a seized phone (including video recordings) was declared inadmissible, on the grounds that the examination of the data was contrary to constitutional guarantees of privacy. The issue was also widely discussed in the television program *“Betimi për Drejtësi”* and at a roundtable organized during *“Anti-Corruption Week 2025”*, where differing views were expressed on the same topic.

The Kosovo Law Institute (KLI) has responded to this debate with the present analysis, in which it examined: (i) the legal basis of the Criminal Procedure Code of the Republic of Kosovo (CPCRK) regarding the seizure and examination of computer devices; (ii) the distinction between interception as a special investigative measure and the administration of evidence obtained from seized devices; (iii) the compatibility of these provisions with Article 36 of the Constitution; and (iv) their compatibility with the case-law of the European Court of Human Rights (ECtHR), within the meaning of Article 53 of the Constitution.

The findings of the analysis indicate that, under the CPCRK, exclusive competence to authorize the examination of seized devices lies with the State Prosecutor, while the Court has competence to order the seizure of the device, but not its examination, since there is no legal basis for the Court to issue a decision authorizing such examination. Furthermore, the analysis finds that data extracted from a lawfully seized device do not constitute “interceptions”, because interception is regulated as a special investigative measure (Articles 85 et seq.), whereas seizure and examination of evidence are regulated in other chapters (Articles 103 et seq.), with different logic and safeguards. In this respect, the Constitution requires a court decision for seizure (Article 36(2)) and for interception of communications (Article 36(3)), but not for the administration or examination of lawfully seized evidence. ECtHR jurisprudence likewise distinguishes between secret surveillance and access to computer data, and does not treat prior judicial authorization as an absolute requirement in every instance of the latter, provided that effective safeguards against abuse exist.

Finally, KLI assesses that changing established practice on the basis of the same law produces serious practical consequences: it risks the collapse of cases in which crucial evidence has been obtained in this manner and creates an unworkable situation for the future, because if a judicial decision for examination is required, the Court does not, in fact, have such competence. For this reason, courts should apply the law as it stands, clearly distinguish between interceptions and seized digital evidence, and, in cases of constitutional doubt, refer the matter to the Constitutional Court through the referral mechanism.

## 2. Background of the problem

The issue with the question of competence to authorize the examination of mobile devices became the subject of public debate in connection with the criminal case against former prosecutor Metush Biraj, in which the Basic Court in Prishtina decided to declare inadmissible the evidence obtained from the examination of a seized phone, including a video recording that had served as key evidence for the corruption indictment. The Court justified this decision by claiming that the examination of the data had been carried out in violation of the constitutional guarantees of privacy. This position was perceived as a significant procedural shift, particularly because the legality of this evidence had been examined and accepted in the earlier stages of the proceedings.

The case and the legal dilemmas it raised were widely discussed both in the investigative television program *Betimi për Drejtësi* and at a public roundtable organized by KLI during *Anti-Corruption Week 2025*, with the participation of prosecutors, judges, lawyers, and criminal law experts. In these discussions, opposing views emerged: one side emphasized that once a device has been seized on the basis of a court order, its examination for investigative purposes falls within the competence of the prosecutor, and that any other interpretation seriously risks undermining criminal investigations. On the other hand, it was argued that access to the contents of a phone constitutes an interference with an individual's privacy and therefore requires a special judicial order.

The debate largely confirmed one fact, namely that the law authorizes the State Prosecutor—and not the Court—to issue orders for the examination of computer devices. In addition to this legal clarity, the research found that the practice followed for many years, including in pending cases, was precisely such: devices were seized by court order, while their examination was authorized by the State Prosecutor. Nevertheless, doubts were raised as to whether these legal provisions are in conformity with the Constitution.<sup>1</sup>

In this regard, as elaborated below, KLI's analysis finds that under the Criminal Procedure Code of the Republic of Kosovo (CPCRK), exclusive competence to authorize the examination of a mobile device lies with the State Prosecutor. Furthermore, the analysis finds that these provisions of the CPRK are fully compatible with the Constitution of the Republic of Kosovo, both through interpretation of its text and through interpretation of that text in the light of the jurisprudence of the European Court of Human Rights (ECtHR).

---

<sup>1</sup> "Examination of a Mobile Phone: Alleged Legal Violations by the Court in the Case of a Prosecutor Accused of Corruption" (see: <https://www.youtube.com/live/tPKjzUFbiBo>) also KLI roundtable discussion: KLI Publishes the Report: Performance of the Justice System in the Prosecution and Adjudication of Corruption (See: <https://kli-ks.org/KLI-publikon-raportin-performanca-e-drejtësisë-ne-ndjekjen-dhe-gjykimin-e-korrupsionit/>).

### 3. Court decision for examination of a phone

The subject of analysis in this section is whether, for the inspection of a phone, a court decision for its seizure is sufficient, or whether an additional court decision is required for the examination of the device.

Article 145(2) of the CPCRK provides that: “For computer devices, electronic storage devices or similar devices that have been lawfully obtained through a court order or with consent, the State Prosecutor may authorize a police officer or an expert to examine, analyze and search for information or data contained within computer devices, electronic storage devices or similar devices.”<sup>2</sup>

In the present context, this provision clearly emphasizes that in order for a specific device to be placed under the control of the state authorities, a court order is required, which must comply with the provisions of the relevant chapter (Articles 103-114 of the CPCRK). In the practice of the justice system, devices have indeed been seized on the basis, the provisions in question do not grant the Court any legal authority to decide on the examination of devices, but only their seizure.

In this manner, the examination of the computer device that has been obtained through a court order may, under the CPCRK, be authorized exclusively by the State Prosecutor. For such examinations, the Court is neither required nor empowered to issue a decision, because there is no legal basis for such a decision.

Although the legal provisions on this matter are clear, even conceptually a judicial decision should not be required for the examination of a device. Once the Court has authorized the seizure of a mobile device, it is understood that this has been done for the purposes necessary I criminal proceedings. If a particular device were not presumed to serve the clarification of a criminal case under investigation by the State Prosecutor, the Court would not have authorized its seizure in the first place. the involvement of the Court in every investigative procedural action of the State Prosecutor would alter the role of the Court, making it part of the investigation (the role of the Prosecutor), rather than merely a guardian of the rights of the defendant during the investigative phase.

For these reasons, in such cases, since the devices were seized pursuant to a court decision, the decision to authorize their examination is issued by the State Prosecutor and not by the Court.

---

<sup>2</sup> Article 145.2. Criminal Procedure Code of the Republic of Kosovo.

#### 4. Retroactive interceptions

The Constitutional Court of the Republic of Kosovo, in case KI/113/21 found that “...The Court considers that the retroactive reading of SMS messages through Order [PP: 51/2014] of the Basic Court in Prizren, of 10 March 2014, violated the applicant’s right guaranteed by Article 36 [Right to Privacy] of the Constitution, and Article 8 [Right to respect for private and family life] of the ECHR.”<sup>3</sup>

The situation described in this judgment concerns the retroactive interception of communications. In other words, the essence of this judgment emphasizes that **interception may be carried out** only from the moment a court decision is issued onwards, but not by going back into the past. The reason for this limitation, according to the Constitutional Court, is the fact that such a possibility is not provided for by law. The exclusive subject matter of this judgment is therefore the *moment of interception*, which under the law may only relate to the future and not to the past, and in no way concerns the administration of evidence already obtained.

In this case, the Constitutional Court did not address the issue of the absence of a judicial decision as such, but rather emphasized that there was no legal basis for issuing such a decision. For this reason, in the context of the subject of this analysis, this case has no relevance, since the object of the analysis is the distinction between interception and the administration of evidence contained in computer devices, and not access to retroactive interceptions.

#### 5. Are materials found on a phone interception?

In line with the subject of this analysis, it must be examined whether the evidence found in an electronic device, lawfully seized and examined on the basis of the prosecutor’s authorization, constitutes “interception”.

“Interception”, according to Article 85 of the Criminal Procedure Code of the Republic of Kosovo (CPRK), is a special investigative measure. This provision lists all special investigative measures in this context, including: secret photographic or video surveillance, covert monitoring of conversations, control of postal shipments, recording of telephone calls, and others.<sup>4</sup> From Article 85 to Article 102, the CPRK regulates the manner in which these measures are applied. In none of these cases is there any reference to the seizure of devices or their examination, but only to special investigative measures. Indeed, within these provisions, the concept of examination is not mentioned in any context. Conceptually, the distinction lies in the fact that in interception

---

<sup>3</sup> Court Judgement in case KI113/21. Constitutional Court of the Republic of Kosovo. Issued 05.01.2022. (See: [https://gjk-ks.org/ep-content/uploads/2022/01/KI\\_113\\_21\\_agj\\_shq.pdf](https://gjk-ks.org/ep-content/uploads/2022/01/KI_113_21_agj_shq.pdf)).

<sup>4</sup> Article 85. Criminal Procedure Code of the Republic of Kosovo.



one obtains data from something that one does not possess, whereas in examination one extracts evidence from something that one lawfully possesses.<sup>5</sup>

By contrast, once the legal regulation of special investigative measures ends (Articles 85–102), Articles 103 and onwards regulate the seizure and examination of seized objects. Thus, in the present case, from a legal standpoint, data extracted from a device seized pursuant to Articles 103 and onwards have nothing to do with “interception” within the meaning given to that term by Article 85 of the CPCRK.<sup>6</sup>

In other words, the provisions on special investigative measures governing “interception” cannot be applied to the collection and examination of seized evidence, the procedures for which were elaborated in the previous chapter.

Therefore, data extracted from a mobile phone do not constitute interceptions.

## 6. Constitutional compatibility of the provisions

The distinction between the provisions of the CPCRK regarding “interceptions” and the examination of devices is also in full conformity with the Constitution of the Republic of Kosovo.

Article 36 of the Constitution of the Republic of Kosovo, paragraph 2, provides that: “Searches of any dwelling or any other private premises, which are deemed **necessary** for the investigation of a crime, may be conducted only to the extent necessary and **only after authorization by the court**, following an explanation of the reasons why such a search is necessary. Deviation from this rule is permitted if it is necessary for a lawful arrest, for the **collection of evidence that is at risk of being lost**, or for the elimination of an immediate and serious danger to persons or property, in the manner provided by law. The court **shall approve such actions retroactively**.”<sup>7</sup>

This provision does not concern “correspondence”. Rather, it refers to the search of a dwelling or private premises and the collection of evidence necessary for a criminal investigation. For the collection of such evidence, the Constitution requires a judicial decision, but not for its administration or examination. In other words, under this provision, the Constitution **protects the citizen from actions without a court decision up to the moment when objects are seized, but not at the stage of their examination**.

By contrast, paragraph 3 of Article 36 of the Constitution provides that: “**The secrecy of correspondence, telephony, and other communications** is an inviolable right. This right may be limited only temporarily, on the basis of a court decision, if it is necessary for the conduct of criminal proceedings or for the protection of the country, in the manner provided by law.” Unlike

---

<sup>5</sup> Article 85-102. Criminal Procedure Code of the Republic of Kosovo.

<sup>6</sup> Article 103-114. Ibid

<sup>7</sup> Article 36.2. Constitution of the Republic of Kosovo.

paragraph 2, this provision explicitly emphasizes the necessity of a judicial decision for limiting the secrecy of correspondence, telephony, and other communications. Thus, this provision concerns the protection of communications in real time, but not evidence obtained from objects seized pursuant to a court decision. In relation to this field, the Constitution always requires a judicial decision.<sup>8</sup>

In line with the distinction between “interception” and the seizure and examination of evidence obtained by a court order, as elaborated in the previous chapter, it follows that the provisions of the CPRK are fully compatible with the Constitution. This is because they require a judicial decision in every case of interception, whereas for other forms of evidence a judicial decision is required only for their seizure, and not for their examination.

## 7. Compatibility of the provisions with the jurisprudence of the ECtHR

According to the Constitution [Article 53], *“Human rights and fundamental freedoms guaranteed by this Constitution shall be interpreted in harmony with the judicial decisions of the European Court of Human Rights.”* Thus, when assessing the compatibility of legal provisions with the Constitution, as done above, the Constitution requires that such compatibility be analyzed in light of how the ECtHR has interpreted human rights and fundamental freedoms.<sup>9</sup>

As explained in the previous chapters, the provisions of the Criminal Procedure Code of the Republic of Kosovo (CPRK) make a clear legal, structural, and conceptual distinction between interception and the examination of evidence, including the stages at which judicial authorization is required. While the provisions governing interceptions always require a judicial decision, in accordance with paragraph 3 of Article 36 of the Constitution, in the case of seized evidence the same judicial decision is required only for the seizure of the objects, and not for their examination, in accordance with paragraph 2 of Article 36 of the Constitution. This conceptual distinction has also been drawn by the ECtHR in its case-law.

In its jurisprudence, the ECtHR clearly distinguishes between interception and the examination of evidence. The fundamental distinction made by the ECtHR relates to whether the interference occurs during the communication process or after its completion.

In the case of *Klass and Others v. Germany*, the ECtHR addressed **the powers of secret surveillance over citizens**,<sup>10</sup> and proceeded to examine the merits of the specific case. Whereas in the case of *Trabajo Rueda v. Spain*, the ECtHR addressed the **seizure of the applicant’s personal**

---

<sup>8</sup> Article 36.3. Constitution of the Republic of Kosovo.

<sup>9</sup> Article 53. Ibid.

<sup>10</sup> *Klass and Others v. Germany*, Application No. 5029/71, Judgment of 6 September 1978, paragraph 42.; Szabó and Vissy v. Hungary, Application No. 37138/14, Judgment of 12 January 2016, paragraph 72–73.  
<https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-57510%22%7D>

**computer**,<sup>11</sup> and proceeded to examine the merits of that case. Thus, the ECtHR itself, in dealing with specific cases, has drawn a clear distinction—also in terminological terms—between surveillance (in our case, interception) and the seizure of computers (in our case, their examination).

The distinction in this respect is not merely terminological. The ECtHR applies different standards of protection to surveillance (interception) compared to access to computer data. With regard to interceptions, the ECtHR has emphasized that: “In the context of secret surveillance measures, review and supervision of such measures may be carried out at three stages: when the surveillance is first authorized, during its execution, or after its termination. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be carried out without the individual’s knowledge. Consequently, since the individual is necessarily prevented from seeking an effective legal remedy on his or her own initiative or from taking a direct part in the review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent safeguards for the protection of the individual’s rights. In a field where abuse is potentially easy in individual cases and where the consequences may be particularly damaging for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, as judicial control offers the best guarantees of independence, impartiality, and a proper procedure.”<sup>12</sup>

With respect to computer data, the European Court of Human Rights (ECtHR) has emphasized that inspections conducted in business premises for the collection of material evidence raise questions regarding the protection of such data from the perspective of the right to respect for “correspondence” and “home,” as guaranteed by Article 8 of the European Convention. For example, in *Bernh Larsen Holding AS and Others v. Norway*, the Court found no violation of Article 8 concerning a decision requiring a commercial company to provide a backup copy of all data stored on a server shared with other companies. Although prior judicial authorization was not required, the Court considered the existence of effective and sufficient safeguards against abuse, the interests of the companies and their employees, and the public interest in an effective tax inspection.<sup>13</sup>

Through cases such as these, it is clear that the ECtHR does not uniformly require the existence of a judicial decision for every form of access to computer data. However, as elaborated above, in the context of interceptions, higher protective standards are necessary due to the individual’s

---

<sup>11</sup> *Trabajo Rueda v. Spain*, Application No. 32600/12, Judgment of 30 August 2017; [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-174221%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-174221%22]}).

<sup>12</sup> *Klass and Others v. Germany*, Application No. 5029/71, par. 55, 56, 233; European Court of Human Rights; . [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57510%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}). *Denysyuk and Others v. Ukraine*, Applications No. 22790/19 et al., par. 88; <https://hudoc.echr.coe.int/eng?i=001-241747>.

<sup>13</sup> *Bernh Larsen Holding AS and Other vs Norway*. Application no.24117/08, Judgment on 15 March 2013, paragraphs 104-175. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-117133%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-117133%22]}).

lack of knowledge that they are being monitored. For this reason, the ECtHR has emphasized that in principle, such measures should be supervised by a judge.

Lower standards of protection apply to access to computer data when its administration occurs with the knowledge of the person that the devices are in the hands of judicial authorities. Nevertheless, even in this second scenario, adequate safeguards must still be provided for citizens.

The Constitution of the Republic of Kosovo similarly makes the judicial decision mandatory for the lawful seizure of an item (in this case, computer devices), but not for their examination. Conversely, a judicial decision is required for the implementation of interceptions. This division is also reflected in the CPRK, which requires a judicial decision for all interceptions, while for other evidence, including computer devices, a judicial decision is needed only for their seizure; authorization from the State Prosecutor suffices for their examination.

Even during the examination of computer devices, the measures taken must be proportionate to the purpose and limited to what is strictly necessary. The Prosecutor's right to examine computer devices does not imply the possibility of data abuse. The lawfulness of procedural actions is assessed at multiple stages, whether in the pre-trial phase or during review and adjudication of the indictment. Normally, if the State Prosecutor fails to comply with legal provisions when examining computer devices, such evidence will be declared inadmissible.

From the above, it follows that the distinction established by the ECtHR is neither incidental nor merely terminological, but fundamentally conceptual.

Given that the jurisprudence of the ECtHR, the Constitution, and the CPRK draw a clear legal, logical, and conceptual distinction between interception and access to computer device data, it is evident that the two categories of evidence do not enjoy the same protection. Accordingly, the Constitution, interpreted in light of ECtHR jurisprudence, requires a judicial decision for interceptions, a judicial decision for the seizure of evidence, including electronic devices, but not for their examination. In the latter case, the ECtHR jurisprudence requires only protective mechanisms, which are provided for under the CPRK. Thus, the provisions of the CPRK authorizing the State Prosecutor to examine evidence seized pursuant to a court order are constitutional, even under an interpretation of the Constitution through the lens of ECtHR jurisprudence.

## 8. Avoidance of applying a law in contravention of the Constitution

As elaborated in the previous chapter, the provisions of the CPRK are fully compatible with the Constitution. Even if a regular court disagrees with this assessment, it cannot avoid applying a law that is constitutional or directly invoke the Constitution in place of the law.

Article 113(8) of the Constitution of the Republic of Kosovo provides that courts have the right to refer a question to the Constitutional Court regarding the constitutionality of a law if the issue

arises during judicial proceedings and the referring court is uncertain about the compatibility of the law with the Constitution, and if the decision in the case depends on the constitutionality of the law in question.<sup>14</sup> Accordingly, if a court has doubts regarding the constitutionality of certain CPRK provisions, it must refer the matter to the Constitutional Court for review, and only after the Court's decision may it proceed with the case.

This principle has been confirmed by Constitutional Court practice. For example, in its decision AA. Uzh.nr.16/2017, of 19 September 2017, the Court emphasized that the Supreme Court had neither interpreted a legal provision (specifically Article 29.1(q) of the Law on General Elections in relation to the restrictions provided in Articles 45, 55, and 71 of the Constitution), nor referred the question of its constitutionality to the Constitutional Court. The Constitutional Court noted that the Supreme Court could have referred the issue to the Constitutional Court pursuant to Article 113(8) [Jurisdiction and Authorized Parties] of the Constitution.<sup>15</sup>

In this decision, the Constitutional Court draws attention to its practice, where it has clarified that, despite the fact that the Constitution grants regular courts the competence to interpret a law-level norm in harmony with a constitutional-level norm and/or to directly apply a constitutional-level norm, this does not mean that regular courts may determine or declare a law-level norm to be in conflict with the Constitution [...] Such a right is granted by the Constitution exclusively to the Constitutional Court.<sup>16</sup>

In a prior case, the Constitutional Court had emphasized that: The Court strongly reiterated that the competence to determine the unconstitutionality of a legal provision and to annul a legal provision as incompatible with the Constitution is an exclusive competence of the Constitutional Court. Thus, despite the fact that the Constitution grants regular courts the authority to interpret a legal norm of statutory rank in harmony with a constitutional provision and/or to directly apply a constitutional norm, this does not mean that regular courts may determine or declare a legal provision as inconsistent with the Constitution or the ECHR. Such a competence—the authority to determine unconstitutionality and to annul a legal provision—is not foreseen by the Constitution as a competence of regular courts. This authority is granted exclusively to the Constitutional Court, which, upon submission of a request by an authorized party under Article 113 of the Constitution, may annul a legal provision found to be inconsistent with the Constitution and determine the effects of such annulment.<sup>17</sup>

Accordingly, avoiding the application of a law on the grounds that it is unconstitutional, without submitting the law in question—such as the CPRK in this case—to the Constitutional Court, constitutes a violation by the court.

---

<sup>14</sup> Article 113.8. Constitution of the Republic of Kosovo.

<sup>15</sup> Constitutional Court of the Republic of Kosovo, Judgment in Case KO95/20, 6 January 2021, par.200. (See: [https://gjk-ks.org/wp-content/uploads/2021/01/ko\\_95\\_20\\_agj\\_shq.pdf](https://gjk-ks.org/wp-content/uploads/2021/01/ko_95_20_agj_shq.pdf)).

<sup>16</sup> Ibid, par. 202.

<sup>17</sup> Constitutional Court of the Republic of Kosovo, Judgment in Case KI207/19, dated 5 January 2021, paragraph 259. (See: [https://gjk-ks.org/wp-content/uploads/2021/01/ko\\_95\\_20\\_agj\\_shq.pdf](https://gjk-ks.org/wp-content/uploads/2021/01/ko_95_20_agj_shq.pdf)).

## 9. Practical consequences

As mentioned above, the legal provisions are clear. On the basis of these provisions, judicial practice has also been established, a practice that has been followed for many consecutive years. Many cases have been investigated, tried and concluded precisely on this legal basis: the devices were seized by a Court decision, while their examination was authorized by the State Prosecutor, in full compliance with the CPRK and with the procedural role of each institution.

However, if judicial practice is changed based on the same law, this produces direct and serious consequences in practice, in two dimensions. The first dimension related to the fact that all cases in which crucial evidence was secured through the examination of computer devices in this manner fail evidence that is based in the law and confirmed so far by judicial practice. The second dimension is even more problematic: if it is claimed that a Court decision is required for the examination of these devices, then a situation arises in which such competence does not exist at all. There is a legal provision granting the court the right to issue ss decision for the examination of computer devices. As a result, even in the future, such evidence cannot be generated, making it impossible to investigate many criminal offenses and, in practice, leading to their de facto amnesty.

Such an approach creates a legal vacuum with serious negative effects: for the past, where citizens have been convicted based on this evidence; for the present, where specific cases are at risk of failing; and for the future, where a large number of criminal offenses will not be investigable at all.

All of this, potentially, is based on a misinterpretation of the law, or on a misinterpretation of its constitutional reading, a dimension that has been sufficiently elaborated in this analysis.

## 10. Conclusions

**Competence:** The competence to authorize the examination of seized telephone devices belongs exclusively to the State Prosecutor, according to the CPRK.

**Court:** The Court has competence only for the seizure of devices, but not for their examination. There is no legal basis for the Court to issue a decision for examination.

**Distinction:** There is a clear legal and conceptual distinction between interception as a special investigative measure and the examination of evidence obtained from seized devices.

**Interception:** Interception concerns real-time communications and always requires a court decision.

**Examination of computer devices:** Data extracted from a lawfully seized device is not interception and is not subject to the rules governing special investigative measures.

**Constitution:** Article 36 of the Constitution requires a court decision for the seizure of items and wiretapping, but not for the administration or examination of seized evidence.

**ECHR:** The jurisprudence of the European Court of Human Rights (ECHR) makes a clear distinction between secret surveillance and access to computer data, with different protective standards for each.

**Constitutional control:** In cases of doubt regarding the constitutionality of the CPRK, the Court should address the Constitutional Court rather than avoid applying the law.

**Practice:** Changing practice under the same law creates uncertainty in the criminal field and risks the failure of criminal cases.

**Consequences:** If the CPRK is not applied in this area, a legal vacuum is created where doubts arise about the legality of past cases, current cases fail, and future cases cannot be investigated under this framework.

## 11. Recommendations

**Application of the Law:** Courts must apply the law as it is, without replacing it with interpretations outside the legal basis.

**Conceptual Distinction:** Courts must clearly understand the distinction between interception as a special investigative measure and the examination of evidence obtained from seized devices.

**Constitutional Compliance:** Courts must interpret the law in harmony with the Constitution as a whole and in the spirit of the ECHR jurisprudence, without limiting themselves to a single paragraph.

**Constitutional Dilemma:** In case of doubt regarding the constitutionality of legal provisions, courts must refer the matter to the Constitutional Court.

