The Legal Framework Governing the Use of Digital Forensic Tools

This document examines the legal framework of the Republic of Serbia governing the use of digital forensic tools (DFTs) and identifies the circumstances in which their deployment may amount to abuse. The analysis draws on a case study based on a report by the international organisation Amnesty International, which presents evidence concerning the use of the Cellebrite digital forensic tool.[1] While the analysis focuses on a specific tool and a specific set of facts, the conclusions reached have broader relevance and apply to all digital forensic tools with comparable or similar functionalities.

At the outset, it should be noted that Serbian law does not recognise "digital forensic tools" (DFTs) as a distinct legal concept. In this document, the term is used to refer to *technical means and software solutions that enable competent authorities to access protected digital devices – such as mobile phones, computers, and other electronic systems – and to extract and analyse data stored on them*.

Although these tools are not expressly regulated as such, their use can be assessed through the existing provisions of the Code of Criminal Procedure (CCP) and the Law on the Police, which establish the evidentiary and investigative measures available to competent authorities for the detection and prosecution of criminal offences.

Moreover, the relevant provisions of the aforementioned laws do not generally address investigative measures directed specifically at devices such as mobile phones and computers, which the CCP classifies as devices for automatic data processing. As a result, determining how these provisions apply to such devices requires an additional layer of interpretation and the contextual application of general rules.

Of particular relevance to this analysis is the way in which the Code of Criminal Procedure treats devices for automatic data processing, placing them in a category that enjoys a particularly high level of protection. This follows from the provisions of the CCP governing searches as evidentiary measures.

The Code distinguishes between searches of homes and other premises, searches of persons, and searches of devices for automatic data processing. As a general rule, a court

[1] Amnesty International, *"A Digital Prison": Surveillance and the suppression of civil society in Serbia*, https://www.amnesty.org/en/documents/eur70/8813/2024/en/

order is required to carry out any search. However, while the law provides for certain exceptions to this requirement in the case of searches of persons or premises, no such exceptions exist with respect to devices for automatic data processing.

An analysis of the relevant evidentiary and investigative measures provided for under the applicable legislation leads to the conclusion that the existing legal framework does not authorise the use of DFTs outside criminal proceedings, nor does it permit their deployment in the absence of a court order.

In practice, the only lawful basis for the use of DFTs is a search as an investigative measure. The execution of this measure is subject not only to a mandatory court order, but also to a set of procedural safeguards, including the presence of a lawyer where requested by the person concerned, comprehensive and precise documentation of the procedure, and strict adherence to the limits set out in the court order. **Any use of DFTs outside this framework constitutes an abuse of authority and a serious violation of fundamental rights**.

Legal Analysis

The analysis draws on a report by the international organisation Amnesty International as a case study, which documents the use of Cellebrite digital forensic tools. In the cases examined, the deployment of these tools was found to be unlawful, as it occurred in the absence of a court order authorising a search and outside the context of any criminal proceedings.

The purpose of examining the relevant investigative measures is to demonstrate that, under the existing legal framework, the use of DFTs can be lawful only where it is based on a court decision and carried out within criminal proceedings. Any use beyond these conditions constitutes an excess of authority and a violation of fundamental rights. On this basis, the analysis links each relevant investigative measure to the potential use of digital forensic tools, drawing on the applicable legal framework and judicial practice in order to delineate the circumstances in which their use is permitted and those in which it amounts to an abuse of power.

On that basis, the analysis focuses on the following investigative measures available to the competent authorities: police checks, the collection of information from citizens, investigative activities, and searches.

1. Police checks (Law on the Police)

Under the Law on the Police, a police officer is authorised to stop and carry out a check of a person, a vehicle, or items carried by that person in a number of specified situations. These include cases where it is necessary to detain the individual, where there is a need to identify objects that could be used for an attack or for self-harm, where measures are being taken to locate persons or objects, or where other actions are carried out in accordance with the Code of Criminal Procedure.[2] The application of this measure does not require a court order.

A key interpretative issue arises in relation to the notion of a police check of movable property. It remains unclear whether such a check is limited to the physical examination of an item, or whether it may also extend to access to its contents. This distinction is particularly significant in the case of devices for automatic data processing, where the primary value lies in the data they contain. The law does not clarify the scope of a police check when applied to this category of devices.

Further legal uncertainty arises from the provision authorising a police officer to forcibly open a closed item carried by a person.[3] Read broadly, this wording could be interpreted as extending to the forced unlocking of devices for automatic data processing. However, such an interpretation would be inconsistent with the structure and purpose of the law.

This power may be exercised without a court order, whereas devices for automatic data processing are afforded a heightened level of legal protection compared to other movable or immovable property. Against that background, the authorisation to forcibly open an item can only be understood as referring to the physical opening of a container or casing. It cannot be construed as permitting forced access to the digital content of a device, which would require a higher level of legal justification and judicial authorisation.

Case law

According to a judgment of the Court of Appeal in Kragujevac (Kž1 710/2019, 15 October 2019), the review of SMS messages stored on a modern mobile phone cannot be treated as an investigative measure relating to movable property. Owing to their complexity, technical characteristics, and multiple functions, mobile phones are considered devices for automatic data processing. As such, their search requires a court order pursuant to Article 152(3) of the Code of Criminal Procedure.

---

[2] Law on the Police, Article 197
[3] Law on the Police, Article 197(8)

The Court further held that the content of SMS messages obtained from the defendant's mobile phone and presented by a police officer through photo-documentation did not constitute a lawful examination of movable property, as the trial court had erroneously concluded. Rather, accessing the content of a mobile phone amounts to a search of a device for automatic data processing, which may be carried out only on the basis of a court order, in accordance with Article 152(3) of the CCP.

In light of the above, the Law on the Police does not provide a legal basis for the use of DFTs by the competent authorities.

2. Collection of information from citizens (Code of Criminal Procedure)

Under the CCP, the police may summon citizens for the purpose of collecting information. The summons must specify both the reason for the request and the capacity in which the person is being summoned.[4]

This measure primarily serves to inform the public prosecutor's assessment of whether and how to proceed further in a given case. In a significant number of instances, individuals from whom information is collected at this stage are subsequently called to testify as witnesses in criminal proceedings.

The summons issued for the purpose of collecting information must clearly state both the reason for the summons and the capacity in which the individual is being summoned. Where the police collect information from a person in respect of whom there are reasonable grounds to suspect the commission of a criminal offence, that person may be summoned only in the capacity of a suspect.[5]

In the context of collecting information from citizens, the use of DFTs to access or unlock a device for automatic data processing is not justified, as this procedure is limited to the taking of oral statements. Moreover, where a person is summoned in the capacity of a citizen – meaning that they are not a suspect and that criminal proceedings have not been initiated against them (in which case they would have to be formally designated as a suspect and informed of the rights that attach to that status)[6] – there are no legal grounds for the use of digital forensic tools.

[4] Code of Criminal Procedure, Article 288
[5] Code of Criminal Procedure, Article 289
[6] Ibid.

3. Scene examination (Code of Criminal Procedure)

A scene examination is conducted where direct observation is necessary in order to establish or clarify facts relevant to the proceedings. The subject of a scene examination may be a person, an object, or a place.[7] It may be carried out in relation to movable and immovable property. In such cases, individuals are required to grant the competent authority access to relevant items and to provide necessary information, and movable property may be temporarily seized under the conditions prescribed by law.[8]

A court order is not required to carry out a scene examination. Such an examination may be conducted where it is necessary to establish or clarify facts relevant to criminal proceedings through direct observation, primarily by visual examination of a device.

The provisions governing the examination of objects further provide that, where entry into buildings, homes, or other premises is required, the rules applicable to searches under the Code of Criminal Procedure must be followed. When this is read together with the technical complexity of devices for automatic data processing – which, in terms of the volume and sensitivity of private information they contain, may be regarded as the digital equivalent of a home – and the fact that a court order is always required to search such devices, it follows that the use of DFTs cannot be justified within the framework of a scene examination.

Case law

According to the judgment of the Court of Appeal in Kragujevac (Kž1 710/2019, 15 October 2019), the review of SMS messages stored on a modern mobile phone cannot be treated as an examination of movable property. Owing to their complexity, technical characteristics, and multiple functions, mobile phones are classified as devices for automatic data processing, the search of which requires a court order pursuant to Article 152(3) of the Code of Criminal Procedure.

In that judgment, the Court correctly held that access to the contents of a device for automatic data processing may be carried out only by way of a search, which is subject in all cases to prior judicial authorisation.

[7] Code of Criminal Procedure, Article 133
[8] Code of Criminal Procedure, Article 135

4. Search (Code of Criminal Procedure)

A search may be carried out where there are reasonable grounds to believe that the suspect or accused, traces of a criminal offence, or objects relevant to the proceedings will be found. As a general rule, a search is conducted on the basis of a court order, with exceptions being narrowly defined and strictly regulated.

When it comes to devices for automatic data processing – such as mobile phones and computers – the law provides no such exceptions. Searches of these devices may be carried out *only on the basis of a prior court order*.[9]

In addition, the procedural rules governing the search of a home or other premises also apply to the search of devices for automatic data processing. These include the mandatory presence of witnesses, the drawing up of an official record, and the right of the person concerned to the full range of procedural safeguards. During a search, items and documents that may serve as evidence may be temporarily seized. Under the law, data stored on a device are likewise regarded as documents for these purposes.

It follows that the use of digital forensic tools is lawful only within the framework of a search as an investigative measure. Their deployment must be based on a court order and carried out in the context of criminal proceedings, with strict observance of procedural safeguards. These include respect for the right to privacy, the right to the presence of a lawyer where requested by the person concerned, and the obligation to ensure accurate and comprehensive documentation of all actions undertaken and evidence obtained.

[9] Code of Criminal Procedure, Article 152