Is Spyware Use Legal in Serbia? An Analysis of the National Legal Framework

In recent years, both domestic and international organisations have documented multiple cases of the use, or attempted use, of spyware in Serbia. These reports provide detailed accounts of the intrusive nature of such tools and the serious risks their deployment poses to fundamental human rights. Notably, Amnesty International has presented evidence indicating that the Serbian police and members of the Security and Information Agency (BIA) have used spyware, referred to in the report as NoviSpy, against activists, journalists, and civil society actors.

Despite the gravity of these findings, questions of legality have so far received limited attention and remain largely peripheral in public debate, including within Serbia's legal community. This analysis seeks to address that gap by examining the national legal framework governing the use of spyware in Serbia and assessing whether such practices have a clear and lawful basis.

Spyware is a form of malicious technology that compromises the integrity of a device and the data stored on it without the user's free and informed consent. It is typically installed covertly, either by exploiting technical vulnerabilities in the device or by deceiving the user, and once deployed it allows for remote control of the infected system.

Because spyware interferes with data and software on a targeted device, it can be classified as a specific category of computer virus. Under Serbia's Criminal Code, computer viruses are defined as computer programs or sets of commands that affect other programs or data within a computer or computer network. What distinguishes spyware from other forms of malware, however, is its primary purpose: the covert surveillance of the user and their communications.

The mere introduction of such software into another person's device constitutes a criminal offence under Serbian law. Its subsequent use necessarily entails unauthorised access to all data stored on the device. This not only intentionally harms the targeted individual, but also affects third parties whose personal data, communications, or information are contained on the same device.

This analysis examines the Constitution of the Republic of Serbia alongside several key statutes relevant to the protection of fundamental rights and freedoms, including the Criminal Code, the Law on Personal Data Protection, the Code of Criminal Procedure, the Law on the Police, the Law on the Security and Information Agency, and the Law on the Military Security Agency and the Military Intelligence Agency.

While Serbian law does not explicitly regulate spyware as a distinct legal concept, a systematic interpretation of the existing legal provisions – when applied to the core functions and effects of such software – leads to the conclusion that the use of spyware lacks a lawful basis and is therefore illegal.

The **Constitution of the Republic of Serbia** provides the foundational guarantees for the protection of privacy and personal data. Article 41 establishes *the inviolability of the confidentiality of letters and other forms of communication*, while Article 42 guarantees the *protection of personal data*.

The Constitution allows for derogations from these protections only in strictly limited circumstances, namely where such interference is necessary for the conduct of criminal proceedings or for the protection of the security of the Republic of Serbia, and only in a manner prescribed by law.

The most explicit criminal law prohibitions relevant to the use of spyware are found in the **Criminal Code**. Article 300 criminalises the creation of a *computer virus* where it is intended to be introduced into another person's computer or network. It also establishes criminal liability where a computer virus is actually introduced into another person's computer or network and causes damage, with penalties including fines and imprisonment.

Article 302 further criminalises *unauthorised access to a protected computer, computer network, or electronic data processing system*, again providing for both fines and custodial sentences. In addition, Article 304a criminalises the production, sale, procurement for use, import, distribution, or any other form of making available devices, computer programs, codes, or data designed to enable access to computers or their components where there is intent for such tools to be used in crimes against computer data or computer systems.

The **Law on Personal Data Protection** provides that processing carried out by competent authorities for specific purposes – such as the prevention, investigation, and detection of criminal offences, the prosecution of offenders, the execution of criminal sanctions, and the protection against threats to public and national security – is lawful only under strict

conditions. Such processing must be necessary for the performance of official duties and must be explicitly prescribed by law, which must in turn define at least the objectives of the processing, the categories of personal data involved, and the purposes for which the data are processed.[1]

This establishes a cumulative set of requirements: *the processing must be necessary, it must have a clear legal basis, and it must be further specified in terms of both purpose and scope*. Given the availability of established investigative and surveillance measures under criminal procedure law – which are significantly less intrusive – the requirement of necessity cannot be met where spyware is used.

Moreover, spyware constitutes one of the most intrusive forms of data processing, due to both the volume and sensitivity of the data it enables access to, as well as the fundamentally non-selective nature of its operation. For these reasons, its use cannot satisfy the proportionality requirement that underpins the personal data protection framework. Finally, the indiscriminate character of spyware means that, in targeting one individual's device, the personal data of third parties whose information is stored on that device are inevitably processed, further undermining its lawfulness under data protection standards.

Under the **Code of Criminal Procedure**, special investigative measures may be ordered against a person where there are reasonable grounds to suspect that they have committed, or are preparing, a criminal offence. Such measures are permitted *only where evidence cannot be obtained by other means*, or where doing so would be significantly more difficult. In deciding whether to authorise such measures, and for how long, the competent authority is required to assess in particular *whether the same objective could be achieved through less rights-restrictive means*.[2]

On the basis of a reasoned request by the public prosecutor, a court may authorise the covert monitoring and recording of a suspect in order to identify their contacts or communications, whether in public places, places with restricted access, or within other premises, with the *explicit exception of the home*.[3] The law's prohibition of covert surveillance in an apartment reflects the heightened level of privacy protection afforded to that space. A comparable level of protection should apply to personal devices such as mobile phones and computers.

[1] Law on Personal Data Protection, Article 13
[2] Code of Criminal Procedure, Articles 161 and 168
[3] Code of Criminal Procedure, Article 171

These devices routinely contain information that is as intimate and sensitive as that kept within a private residence, including personal documents, photographs, private communications, and other highly personal data. For this reason, phones and computers may be understood as the digital equivalent of a home: a personal space in which individuals are entitled to the fullest protection of their privacy. The deployment of highly intrusive tools such as spyware therefore constitutes an impermissible interference with privacy and fundamental rights.

Even the special investigative measure of covert monitoring of communications cannot justify the use of spyware. While such measures are narrowly targeted and limited to communications linked to a specific telephone number,[4] spyware operates at the level of the entire device, granting access to all data it contains. This qualitative difference places spyware well beyond the scope of what criminal procedure law permits.

A further argument against the use of spyware can be drawn from the logic of the Code of Criminal Procedure itself, and in particular from the legislature's approach to special investigative measures that constitute the most far-reaching interferences with citizens' rights recognised in Serbian law. Even these traditional surveillance measures – which are significantly less intrusive and harmful than spyware – are subject to strict substantive and procedural limitations.

They may be authorised *only in relation to the most serious criminal offences*, exhaustively listed by law, and *only where evidence cannot be obtained by other means or where doing so would be substantially more difficult*. In addition, the competent authority is *required, in every individual case, to assess whether the investigative objective can be achieved through measures that entail a lesser interference with fundamental rights*.[5]

Under the **Law on the Police**, police officers may, in certain circumstances, carry out targeted search measures through the use of special investigative measures, subject to the approval of the President of the Supreme Court of Cassation. These measures must, however, be applied in accordance with the Code of Criminal Procedure.[6] As set out above, that framework does not provide a legal basis for the use of spyware, rendering its deployment unjustified and unlawful.

The **Law on the Security and Information Agency** (BIA) permits the application of special measures against an individual, group, or organisation where there are *reasonable grounds to suspect activities aimed at undermining the security of the Republic of Serbia*,

[4] Code of Criminal Procedure, Articles 166-170
[5] Code of Criminal Procedure, Article 161
[6] Law on the Police, Article 60

and where the circumstances indicate that such activities *could not be detected, prevented, or proven by other means*, or only with disproportionate difficulty or significant risk.

In deciding whether to authorise such measures, and for what duration, the law requires an assessment of *whether the same objective could be achieved through less rights-restrictive means, and only to the extent necessary to meet the legitimate aim pursued in a democratic society*.[7]

The special measures available to the BIA allow for derogations from the inviolability of the confidentiality of letters and other forms of communication. These include the covert monitoring and recording of communications, irrespective of the form or technical means used; surveillance of electronic and other addresses; and covert monitoring and recording of communications in public places, in places with restricted access, or within private premises.[8]

Accordingly, the special measures authorised under this law are limited exclusively to communications. As noted above, spyware operates in a fundamentally different and indiscriminate manner: it targets the device as a whole and thereby grants access to all data stored on it. The use of spyware would therefore go beyond the scope of the measures permitted under this law and exceed the limits it prescribes.

The legislature has designed the regime for authorising special measures in a deliberately restrictive manner, despite the fact that these measures are significantly less intrusive and harmful to fundamental rights, as they are limited exclusively to communications. Their use is confined to situations where there are *reasonable grounds to suspect activities directed against the security of the Republic of Serbia*, and where the circumstances indicate that such activities could not otherwise be detected, prevented, or proven, or only with disproportionate difficulty or serious risk. In every individual case, the competent authority must also assess whether the same objective could be achieved through measures that interfere less with the rights of citizens, and only to the extent necessary in a democratic society.

The existence of such a narrowly circumscribed framework for measures that are clearly less intrusive than spyware underscores the absence of any legal justification for the use of spyware. The deployment of such software would constitute a disproportionate and impermissible interference with privacy, affecting not only the individuals directly targeted but also all third parties whose data are stored on or pass through the

[7] Law on the Security and Information Agency, Article 14
[8] Law on the Security and Information Agency, Article 13

compromised device. This exceeds the limits of permissible rights restrictions under Serbian law and leads to the clear conclusion that the legislature would regard such practices as unlawful and unacceptable.

Under the **Law on the Military Security Agency and the Military Intelligence Agency**, the Military Security Agency (VBA) is authorised, within its strictly defined mandate relating to the security and counter-intelligence protection of the Ministry of Defence and the Serbian Armed Forces,[9] to covertly collect data through the use of special procedures and measures. Such measures may be applied *only where the relevant data cannot be obtained by other means*, or where doing so would entail a disproportionate risk to human life, health, or property, or involve disproportionate expense.

Where several special procedures or measures are available, the law *requires the VBA to apply those that least interfere with the human rights and freedoms guaranteed by the Constitution*.[10] It means that the VBA is also bound by the principles of necessity and proportionality in the exercise of its powers.

The applicable legal framework provides clear and consistent grounds for concluding that the use of spyware in the Republic of Serbia cannot be regarded as either lawful or legitimate. Spyware is not explicitly regulated or authorised under existing legislation, and its core functionalities correspond to conduct that is expressly prohibited by law. In particular, the Criminal Code criminalises the acts necessary for the deployment of spyware, including unauthorised access to computers and networks, the creation and use of computer viruses, and the unlawful processing of personal data.

Moreover, special investigative measures and security-service powers – representing the most serious interferences with citizens' rights recognised under Serbian law – are subject to strict requirements of necessity and proportionality and are limited to narrowly defined circumstances involving the most serious offences. The legislature has thus adopted a deliberately restrictive approach even in relation to measures that are significantly less intrusive than spyware. This legislative design confirms the absence of any legal basis for the use of spyware under the Serbian legal framework.

By its very nature, spyware enables comprehensive and indiscriminate control over a device, granting access to all data it contains, including personal documents, photographs, private communications, and the data of third parties. Such access goes far beyond what can be considered a permissible restriction of fundamental rights. Personal devices such as mobile phones and computers, as the digital equivalent of a home, are entitled to a

[9] Law on the Military Security Agency and the Military Intelligence Agency, Article 5
[10] Law on the Military Security Agency and the Military Intelligence Agency, Article 11

heightened level of privacy protection. The indiscriminate collection of data from these devices is therefore incompatible with the constitutional right to privacy and with the principles of necessity and proportionality that underpin the entire system of special investigative measures and security-service powers.

In light of the existing legal framework of the Republic of Serbia, the use of spyware lacks any lawful basis and is incompatible with both statutory safeguards and fundamental human rights. Spyware should therefore be understood not merely as a technical issue, but as a legally and socially unacceptable form of surveillance.