POLICY PAPER / 1

BCSP Belgrade Centre for Security Policy

SPYWARE

THE NEGATION OF HUMAN RIGHTS UNDER THE PRETEXT OF "SECURITY"

Milica Tošić

RECOMMENDATIONS

- **A complete ban** – suspend the development, procurement, testing and use of spyware.
- **Supervision and prosecution of previous cases** – all competent institutions, within their competencies, should carry out procedures to control the legality of actions, as well as to establish responsibility for all previous forms of use of spyware.
- **Mandatory subsequent notification to subjects of monitoring and an effective remedy** – prescribe that every person who has been under monitoring be notified in a timely manner (when such notification cannot jeopardise the investigation) with clear contents of the notification, with strict deadlines and independent oversight, as well as automatic extraction and destruction of illegally obtained data.

January 2026

SUMMARY

The point of departure for this analysis was the idea that spyware by its nature is indiscriminate, comprehensive and covert surveillance tool, structurally incompatible with the principles of necessity, proportionality and targeted data processing. The Constitution, Criminal Procedure Code, Criminal Code and respective laws on intelligence services, electronic communication, personal data protection and information security have already set forth rigorous conditions for conducting secret monitoring, which spyware cannot meet in reality. International standards and comparative practice have confirmed significant differences: massive "collateral" collection of third-person data, privacy undermining, compromising professional secrecy and protection of journalists' sources, abuse of the pretext of "national security" and prevention of effective legal protection due to the secrecy of measures. In Serbia, there are already documented cases of targeting journalists and activists, without any accountability of the persons responsible for that. The conclusion is self-explanatory: urgent prohibition of spyware is needed, as well as the prosecution of the so-far illicit practices.

INTRODUCTION

Spyware is not just another "investigative tool." It is a technique that provides covert, comprehensive access to the entire device, including messages, documents, contacts, location, microphone/camera. Such monitoring is, by its very nature, incompatible with the principles of necessity and proportionality – instead of targeting the specific data of the person under surveillance, it captures almost everything, including the data of many other persons.

The fact that the term "spyware" does not exist in most relevant domestic regulations does not imply a legal vacuum. On the contrary, the Constitution, criminal law provisions, regulations on security services, personal data protection and electronic communication set forth strict conditions for the use of monitoring tools. With all these rules, the use of spyware is in systematic conflict.

The way in which institutions in Serbia have so far reacted to publicly documented allegations that the state is using spyware shows that the system is not ready to legally and safely control such a tool. In countries with democratic capacities more developed than the domestic ones, the demand for a moratorium or ban prevails until extremely strict guarantees are established,[1] thus it is rational to make the same request in Serbia.

The following analysis explains what spyware is (not), provides an overview of relevant domestic legislation, summarizes the cases known so far and the attempts to use it in Serbia, and singles out key risks, which are by international standards and case law.

The conclusion is self-evident – under the current conditions, the use of spyware cannot meet the standards of the rule of law and protection of human rights.

WHAT IS (NOT) SPYWARE?

Currently, Serbia's applicable law does not contain a definition of spyware. However, a detailed description of this term can be found in international regulations, documents of international bodies and reports of international organisations dealing with the protection of human rights.

The Venice Commission[2] uses "spyware"[3] as an umbrella term for intrusive monitoring software, which secretly penetrates devices (e.g. smartphones, computers) without the user's awareness, allows the operator to monitor the location in real time, read data and communication (including bypassing safeguards such as encryption), and take control of the hardware and software of the device (microphone, camera, etc.). In contrast to "classic eavesdropping", such a tool can also provide retroactive access to pre-existing files, messages, passwords and metadata.

The European Media Freedom Act[4] (EMFA) provides a normative definition of "intrusive monitoring software" as a product with digital elements, specifically designed to exploit vulnerabilities in other digital products to enable covert monitoring (monitoring, extraction, collection or analysis of data), even in an indiscriminate form.

One of the most precise definitions is provided by the European Digital Rights Organisation (EDRi),[5] which explains this term operationally and states that "spyware" is considered to be any software that, predominantly by exploiting vulnerabilities, covertly penetrates a device, violates its integrity and thus enables remote monitoring, data collection and/or extraction, and control and/or manipulation of the device. According to this description, in order to speak of spyware, the following characteristics must be cumulatively met: (1) the action is covert, without the knowledge of the user; (2) penetration is achieved through exploitation of vulnerabilities or related techniques of circumvention of protection; and (3) direct access is achieved to the device itself (not only to network traffic), with the possibility of a permanent presence of an "agent". In addition, it is sufficient that at least one of the following functionalities is fulfilled (alternatively): continuous monitoring of activities and/or location; reading and retroactively extracting content and metadata, or remotely controlling device functions and sensors (e.g., microphone/camera activation).

All of the above definitions distinguish spyware from network interfaces for lawful interception of communication and forensic tools, which do not involve secret infection of the device.

LEGISLATION IN SERBIA

Constitution

Understanding spyware in the domestic legal framework starts with the Constitution. The Constitution of the Republic of Serbia[6] guarantees the secrecy of letters and other means of communication and allows derogation only temporarily, on the basis of a court decision, when it is necessary for criminal proceedings or the protection of state security, in the manner envisaged by law.[7] The Constitution also guarantees the protection of personal data.[8] These two norms are the basis of all subsequent restrictions and procedures in the laws governing secret surveillance and access to data.

Criminal Law

According to the Criminal Procedure Code[9], secret surveillance is allowed only as a special evidentiary action and only with a prior court order, issued on the basis of a reasoned motion of the public prosecutor. Special evidentiary action may be introduced only against a person of whom there are grounds for suspicion to have committed

an act that the law identifies as one of the most serious (specifically listing them),[10] provided that the evidence cannot be collected in any other way or its collection would be significantly more difficult. When deciding on the imposition and duration of secret surveillance, the procedural authority is obliged to assess in particular whether the same result could be achieved in a way that less restricts the rights of citizens.[11]

The order must be precise: it shall state the available information on the person under monitoring, the legal name of the criminal offence, the grounds on which the suspicion is based, as well as the manner of implementation, scope and duration of the measure. The basic duration is up to three months, with the possibility of extension for another three months, and for acts under the jurisdiction of special prosecutors, exceptionally, two more times for three months.[12] The order is executed by the police, the Intelligence Agency (hereinafter: BIA) or the Military Intelligence Agency (hereinafter: VBA).[13]

Covert surveillance of communication includes the monitoring and recording of communication carried out by telephone or other technical means, the monitoring of electronic or other addresses, as well as the temporary seizure of letters and correspondence.[14] If, in the course of the measure, it is found out that the suspect is using a different telephone number or address, the monitoring may be temporarily extended, but subsequent approval of the pre-trial judge is required within 48 hours of receipt of the public prosecutor's motion.[15]

Upon completion of the measure, the authority that conducted the monitoring shall submit to the pre-trial judge and the public prosecutor the collected materials (recordings of communication, letters and other items), as well as a special report stating the time of the commencement and end of the monitoring, data on the officer who conducted the monitoring, a description of the means used, data on the persons subjected to the monitoring and an assessment of the expediency and results of the implementation of the monitoring.[16]

If the public prosecutor does not initiate criminal proceedings within six months from the day of getting acquainted with the material or declares the decision not to use the collected materials in the proceedings, the pre-trial judge issues a decision on the destruction of the materials in question. In this situation, the judge may (but does not have to) inform the person who has been under monitoring.[17]

In particular, the Law points out that, if the actions within the undertaking of special evidentiary measures were in contravention of the legal provisions or of the order of the procedural authority, such material shall be considered illegal evidence, a court decision cannot be based on it and the material in question shall be destroyed.[18]

Thus, the legal framework provided by the CPC allows for targeted, selective monitoring of specific data and identifiers, with strict time limits, records and a regime for the destruction of materials. All this is allowed only if the criteria of necessity and

proportionality are met. However, even if we take into account that in a particular case all procedural conditions are met, as well as that monitoring is actually carried out pursuant to a reasoned court order, the technical non-selectivity of spyware, as a rule, does not correspond to these rules and, according to the Criminal Code, raises the question of potential criminal liability.

The Criminal Code[19] (hereinafter: CC) provides protection by listing a number of incriminations relevant to the abuse of monitoring and digital tools, for example – unauthorised wiretapping and recording[20] and unauthorised collection of personal data.[21] Also, there are criminal offences against the security of computer data: damage to computer data and programmes,[22] computer sabotage,[23] making and introducing computer viruses,[24] computer fraud,[25] making, procuring and giving to others the means to commit crimes against the security of computer data.[26]

At the time of writing this analysis, public consultations on the Draft Law on Amendments to the Criminal Procedure Code[27] and the Draft Law on Amendments to the Criminal Code are in progress.[28] The proposed amendments go in three directions that are particularly important in this area. First, the Draft CPC significantly expands the list of offences for which special evidentiary action may be ordered (including secret monitoring),[29] thereby shifting these measures from exception to rule, weakening the standards of necessity and proportionality, and increasing the risk of selective application. Second, the Draft CC changes the term "computer virus" to "malware" ("malicious computer programme),"[30] but the proposed definition relies on subjective elements ("with the intent to cause harm," "with the intent to endanger ..."), which shifts the focus from the objective properties of the tool to proving the intrinsic intent of the perpetrator, reduces legal certainty and aggravates prosecution. Thirdly, it provides for the mandatory subsequent notification of persons who have been the subject of court-ordered measures,[31] which is a step forward, but in order to have a real effect, it must be regulated by strict deadlines, the mandatory content of the notification (legal basis, duration, scope of the concerned data, to whom it was disclosed), as well as the obligation to keep records and destroy illegally obtained data.

Intelligence Services

In addition to the powers emanating from the CPC, the intelligence services may also conduct covert monitoring pursuant to the law governing them. The Law on the Intelligence Agency[32] stipulates that the BIA may take certain special measures derogating from the inviolability of the secrecy of letters and other means of communication, including: 1. secret monitoring and recording of communication, regardless of the form and technical means by which the monitoring of electronic or other addresses is carried out; (b) surreptitious surveillance and recording of communication in public places and places to which access is restricted or on premises; 3. statistical electronic monitoring of communication and information systems in order

to obtain data on the communication or location of the mobile terminal equipment used, and 4. computer search of already processed personal and other data and their comparison with data collected by the application of previous measures.[33]

These measures may be imposed only on a person, group or organisation with grounds for suspicion of undertaking or preparing actions directed against the security of the Republic of Serbia, in situations where these actions cannot be carried out in a manner that is less restrictive of the rights of citizens, and to the extent "necessary to fulfil the purpose of the restriction in a democratic society."[34] All measures are time-bound and are determined by court order upon the proposal of the BIA Director, with a precise indication of the person to whom they will be applied, the existence of conditions for imposition, the manner of application, the scope and the expiration date.[35] Information on proposing the implementation of measures, on decision-making, as well as on their application is classified information.[36]

Similar mechanisms are provided for in the Law on Military Security (VBA) and Military Intelligence Agency (VOA)**.**[37] Within their competences,[38] related to the security protection of the Ministry of Defence and the Serbian Army, the VBA and VOA are allowed to apply a catalogue of "special procedures and measures," including secret monitoring.[39] These measures are carried out on the basis of reasoned orders of the VBA Director or an official of the VBA authorised by the Director[40], or on the basis of reasoned decisions of the court[41].

The security services are secretive in nature, but the complete lack of transparency of their work is incompatible with the legal role assigned to them. And in this regime, the measures they implement must be targeted, time-limited and proportionate, with priority given to less invasive means where possible. Also, they must be based on judicial review and the requirement from the BIA Law that the restrictions are "necessary in a democratic society". Due to the technical non-selectivity of spyware (penetration of the entire device and wide scope of data), its use is in principle incompatible with these standards and potentially leads to the illegality of collected material and the risk of criminal liability.

Electronic Communication

The Law on Electronic Communication[42] (hereinafter: ECL) protects the secrecy of communication and allows for derogation only temporarily, with a court decision, if it is necessary for conducting criminal proceedings or for the protection of the security of the Republic of Serbia, and in the manner set forth by law.[43] The operator shall be obliged to facilitate lawful interception on the basis of such a decision and to provide the necessary devices and software at its own expense.[44] The competent authority and the operator must keep records of each interception (legal basis, date, time) and keep them secret.[45]

The Law on Electronic Communication also regulates retained communication data, which do not reveal the content of the message, but the circumstances of its conveyance (who communicated with whom, when, for how long and by what means) with technical identifiers and location traces, the so-called metadata.[46] The operator shall store them for 12 months, and access to them is allowed only on the basis of the user's consent or on the basis of a court decision for the purpose of conducting criminal proceedings or protecting security.[47]

Technical and organisational details are prescribed by the Rulebook on Requirements for Devices and Software for Lawful Interception of Electronic Communication and Technical Requirements for Fulfilling the Obligation to Retain Data on Electronic Communication.[48] The Regulation defines the necessary technical and organisational conditions, i.e. appropriate devices and software support, which the operator is obliged to provide.[49] It also defines a "monitoring centre" as a location where devices and software for the purpose of lawful interception are located,[50] whereby it is determined that, until a separate body is established, the monitoring centre is located on the premises of the BIA.[51]

It follows from these decisions that the regime is designed for the targeted, networked implementation of lawful interception on the part of the operator and on the basis of an appropriate court decision, and not for the covert infection of users' devices with commercial spyware. Situating the monitoring centre (even temporarily) in the premises of the BIA is not an acceptable solution – the placement of the technical point of execution of court orders in the institution implementing the measures increases the risk of a conflict of interests and weakening of external control.

Personal Data Protection

The Law on Personal Data Protection[52] is a general regulation that governs the processing of personal data, including the processing carried out by the competent authorities for the prevention and detection of criminal offences, the prosecution of perpetrators and the protection of security (the so-called "special purposes").[53]

Any processing of data must comply with the principles of, *inter alia*, lawfulness, purpose limitation, minimisation and proportionality.[54] Processing carried out by competent authorities for "special purposes" is lawful only if it is necessary for the performance of the tasks of the competent authorities and if it is required by law.[55] In these situations, the law prescribes an obligation for the competent authorities to record in detail each use of the automated processing system for the purpose of subsequent verification of legality,[56] as well as technical and organisational security measures commensurate with the risk.[57]

In situations where it is likely that a certain processing operation, especially if it involves the use of new technologies, will pose a high risk to the rights and freedoms of individu-

als, the law prescribes the mandatory implementation of an impact assessment on the protection of personal data, prior to the implementation of data processing.[58]

Bearing in mind that commercial spyware implies indiscriminate and comprehensive access to the device and the personal data that may be contained in it, it is almost impossible to imagine a situation in which such processing is compliant with the principle of minimisation and limitation of the processing purpose. However, even if there were an adequate legal basis in this hypothetical situation, any processing operation using spyware, as well as any acquisition of such equipment, would have to undergo a rigorous impact assessment, to ensure adequate security measures and guarantees of access logs.

Information Security

The newly adopted Law on Information Security[59] (hereinafter: ISL) is a systemic regulation in the field of information security and defines the term "malware,"[60] which explicitly includes spyware. This qualifies spyware as a threat vector and subject to prevention and response measures, rather than as an authorised investigative tool. The Law on Information Security introduces the obligations of entities that manage information and communication systems (risk management, technical and organisational measures, records, reporting of significant incidents to competent authorities/CERT structures) and regulates the coordination of incident procedures. The qualification of spyware as "malicious" confirms that the ISL treats such activity as a security risk, which should be prevented and remedied, and not as a permissible investigative technique.

EXAMPLES OF INTERNATIONAL REGULATIONS

In Germany, the use of spyware is regulated by the Criminal Procedure Code and applies to a strictly limited catalogue of criminal offences. The Federal Constitutional Court has narrowed the scope of "technical infiltration/online searches" to prevent the measures from leading to the findings from the "core of privacy." Technical measures must, as far as possible, avoid the collection of data related to private life. The law explicitly stipulates that spyware measures are impermissible if they lead solely to the findings from the core of privacy. In order to ensure compliance with the standards, such data searches must be subject to prior approval by the Independent Supervisory Board.[61]

In Austria, in 2018, the Criminal Procedure Code introduced a provision that allowed the use of spyware in criminal investigations. The measure was intended to secretly monitor encrypted messages by installing software on a computer or other device (a so-called "state Trojan"). However, these provisions never came into force, as the Constitutional Court declared them unconstitutional on December 11, 2019. The Court held that such

a review constituted a serious interference with the right to privacy enshrined in Article 8 of the European Convention on Human Rights (ECHR) and was permissible only within extremely narrow limits in order to protect equally important legally protected goods. In particular, the Court pointed out the following shortcomings: the measure would affect a large number of persons; there was no guarantee that it would be used solely for the purpose of prosecuting and shedding light on sufficiently serious crimes; The protection of the privacy of those concerned is not adequately ensured; There was no guarantee of effective and independent oversight of the implementation of this measure.[62]

In the Netherlands, a legislative framework is in place regulating the use of spyware in both criminal investigations and intelligence and security purposes. The regulations define methods of data collection, such as determining the identification characteristics of computer systems, intercepting communications, systematic monitoring, obtaining stored data, and making data unavailable. Different conditions apply to each of these methods depending on the severity of the crimes. In 2022, the Centre for Research and Data of the Ministry of Justice and Security published a report stating that spyware was used in 26 criminal investigations between March 2019 and March 2021. The investigations included serious crimes, including murder, narcotics-related offences, money laundering, terrorism and membership of a criminal organisation. In criminal investigations, persons are notified of the use of spyware as soon as possible, unless this is "not reasonably possible" or disclosure would jeopardize the investigation. Intelligence is also required in intelligence and security measures, unless it would jeopardize sources and relations with other countries or reveal working methods.[63]

THE USE IN SERBIA

Available research and news reports show that journalists, activists and members of civil society in Serbia have been targeted by advanced monitoring tools, including commercial spyware as well as domestically developed software. The most comprehensive finding was made by *Amnesty International* in its study "A Digital Prison,"[64] published in December 2024, describing the practice of secretly infecting phones during detention or informative conversations between activists and journalists in the police and the BIA, combined with the use of forensic tools (*Cellebrite*) to forcibly unlock the device and extract data. In several cases, traces of the installation of domestically developed software, named "NoviSpy" by the research team for the purposes of the report, were documented, including system logs and communication with servers connected to the BIA. It has also been documented that the number of concerned devices is likely to be many times higher than the forensically confirmed cases so far.

In early 2025, at least two attempts were verified to infect the phone of a BIRN journalist with commercial spyware called "Pegasus."[65] Although the formal identification of the commissioning authority has not been disclosed, there is a high degree of probability that it is a state actor, as the manufacturer NSO Group officially licenses Pegasus exclusively to state security and law enforcement authorities.[66] In February 2025, *Amnesty International* also documented another attempt to compromise – this time targeting a student activist's phone.[67]

Previous traces of civil society being targeted were also documented at the end of 2023, when two people from the civil sector in Belgrade received warnings from Apple about possible state-sponsored attacks. Forensic findings from several organisations (*Amnesty, Citizen Lab, Access Now*) pointed to techniques previously seen in Pegasus, although the infection was not officially confirmed at the time.[68]

Immediately after the publication of the report "*A Digital Prison*," nine civil society organisations from Serbia sent requests to the relevant domestic and international institutions, namely: (1) criminal charges lodged with the Prosecutor's Office for Cyber Crime against unidentified authorised persons from the BIA and the police;[69] (2) a request to the Commissioner for Information of Public Importance and Personal Data Protection to initiate supervision;[70] (3) addressing the Ombudsman for the purpose of initiating proceedings on his/her own initiative;[71] (4) Addressing the Commissioner for Human Rights of the Council of Europe[72] and the Special Procedures before the United Nations Human Rights Council.

In addition to these institutions, the competence to verify the legality of the actions of the relevant services is vested in the Internal Control Sector of the Ministry of the Interior,[73] the BIA Internal Control,[74] as well as the National Assembly's Committee for the Control of Security Services.[75]

On the date of this writing, according to publicly available sources, there is no confirmation of institutional outcomes or accountability. There are general denials of the allegations or the absence of comments from the authorities, as well as announcements by some commercial suppliers that they will check and implement possible measures[76] following the Amnesty International report, but without confirmation of the formal suspension of the use of their products in Serbia.

WHAT ARE THE RISKS OF USE?

Listed below are some of the risks that accompany each use of spyware, identified in both international documents and case law.

Disproportionality and Violation of the Principle of Necessity

That "the use of spyware goes far beyond and is fundamentally incompatible with the basic legal principles of necessity and proportionality," is one of the main conclusions of EDRi.[77] In addition, the European Court of Human Rights (hereinafter: the Court) interprets the standard "necessary in a democratic society" as "strict necessity," while warning that "any measure of secret monitoring that does not meet the criterion of strict necessity is prone to abuse."[78]

Undermining the Right to Privacy and Family Life

The right to respect for private and family life (Art. 8 of the European Convention on Human Rights) also includes the protection of personal data and correspondence. The European Court of Human Rights emphasises that "the protection of personal data is essential for the enjoyment of the right to respect for private and family life".[79] In the domain of covert surveillance, the Court also found that "the mere existence of legislation permitting the secret monitoring of communications constitutes an interference with the right under Article 8", since it creates a permanent threat of monitoring to anyone to whom it may apply.[80] Such standards are particularly relevant for spyware, as full access to the device, content, metadata, and sensors typically means deep and continuous interference in the private lives and correspondence of family members and close persons.

Excessive Collection and "Collateral" Processing of Third-Party Data

Spyware almost inevitably captures off-target data (contacts, messages, and other data of individuals who are not subject to monitoring) and creates a "surplus of information." The Venice Commission explicitly warns that the use of spyware "can lead to the collection of '*surplus information*', i.e. data irrelevant to a specific investigation," which "poses a particularly serious risk to privacy (...), including persons in the target's environment" and "raises serious questions about the proportionality of any use of *spyware*."[81] Thus, even if we were to assume that the use of spyware to monitor a particular person is lawful and justified, it entails the collateral collection of third-party data on a scale that is legally difficult to justify.

Excessive Use Due to a Broad Interpretation of the Term "National Security"

The term "national security" is often used flexibly, which opens up space for the expansion of covert monitoring beyond the situations for which it is intended. The European Court of Human Rights (ECtHR) ruled in the case of Weber and Saravia v. Germany that there was "a risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it."[82] Also, the Venice Commission emphasizes that "the vagueness of the concept of national security creates special problems" and that the discretion of the executive must not be "unlimited," but "the law must (...) clearly set the limits to such discretion", as well as that "the boundaries of the concept of national security may not be extended beyond its natural meaning."[83]

If we look at the above in the context of Serbia and the traditional "untouchability" of the security services, the problem of the absence of control and supervision of the lawfulness of actions is logically linked to the above.

The "Effect of Anxiety" on Freedom of Expression and the Protection of Journalists' Sources

Spyware undermines confidentiality, which is essential for journalism – without a guarantee of secrecy, sources renounce communication, while journalists self-censor. The European Court of Human Rights has made it clear – "the protection of journalists' sources is one of the basic conditions of free journalism" and courts must bear in mind the "potential anxiety effect" of a source disclosure order.[84] By using spyware, the state abolishes the presumption of confidentiality between journalists and sources, as well as guarantees of freedom of expression.

Violation of Professional Secrecy

As a rule, spyware "enters" the entire device, and therefore interferes with correspondence, documents and communication protected by professional secrecy (attorney's, medical and other). International standards set a very high threshold for protection. The U.N. Basic Principles on the Role of Lawyers require State Parties to "recognise and respect that all communication and consultations between lawyers and clients are confidential."[85] A similar standard applies to medical confidentiality.[86]

Effective Legal Protection Prevented Due to Secrecy and Lack of Information to Victims of Unauthorised Monitoring

The secrecy of monitoring and the absence of subsequent notification mean that the concerned persons never know that they have been subjected to the measures and therefore cannot dispute them. European standards therefore start from the obligation of subsequent notification – according to a summary of the case law in the Venice Commission report, the European Court of Justice requires that the person subjected to the measures "be informed without delay" and "as soon as the provision of information is possible without jeopardising the purpose of the investigation",[87] upon completion of the measures. In the absence of such a notification, there is no effective remedy, as well as no subsequent actions of compensation for the damage caused. As previously stated in the overview of applicable regulations, domestic authorities are not obliged to notify persons that they have been subjected to monitoring, which makes legal protection illusory.

Misuse for Political Purposes

International sources have consistently reported spyware misuse for political purposes. The European Parliament explicitly states that "spyware has been illegally used for the purposes of surveillance of journalists, opposition politicians, lawyers, prosecutors and representatives of the civil sector."[88]

In Serbia, political abuse of institutions is a burning issue even without the use of spyware, and there are no grounds to believe that the same actors would use such a tool legally, proportionately and with effective oversight.

The Lack of Public Oversight and Accountability

Despite serious and consistent allegations of attempted and/or perpetrated infections of the devices of journalists, activists and students, no competent authority in Serbia has publicly taken concrete steps to meet the standards of public oversight and accountability. There are no published results of internal controls in the Ministry of the Interior and the BIA, no information on disciplinary or criminal proceedings initiated against responsible persons, nor a statement from the National Assembly's Committee for the Control of Security Services regarding this situation.

Even though the persons who were under surveillance and civil society organizations have initiated proceedings, to this day we do not know whether the independent institutions, prosecutor's office seized of the matter have taken concrete steps aimed at protecting citizens' rights.

All of the above leaves room for only one conclusion – the domestic regime does not meet the key international requirements for information, oversight and effective remedy.

CONCLUSION

Drawing on numerous international documents and case law, this analysis paints a simple picture: spyware is inherently indiscriminate, comprehensive and covert, and therefore structurally incompatible with the necessity, proportionality, targeting, time limits, and other privacy standards that pervade our legal order. Even if there were a formal legal basis, the spyware technique annuls the safeguards: it undermines the privacy and confidentiality of professional secrecy, thwarts the protection of journalists' sources, and makes any effective remedy virtually impossible due to secrecy and lack of information. Domestic institutional practice further confirms that the system is not ready to control such an invasive tool within the limits of the rule of law.

Therefore, the use of spyware has no legitimate place in a democratic society or in the domestic legal framework. A swift and clear political and legal decision is needed, which stops further use, sheds light on and sanctions the actions taken so far and restores meaningful legal protection to citizens.

RECOMMENDATIONS

- A complete ban – suspend the development, procurement, testing and use of spyware.
- Supervision and prosecution of previous cases – all competent institutions, within their competencies, should carry out procedures to control the legality of actions, as well as to establish responsibility for all previous forms of use of spyware.
- Mandatory subsequent notification to subjects of monitoring and an effective remedy – prescribe that every person who has been under monitoring be notified in a timely manner (when such notification cannot jeopardise the investigation) with clear contents of the notification, with strict deadlines and independent oversight, as well as automatic extraction and destruction of illegally obtained data.

SOURCES AND NOTES

1 For example: Michele Failla, "A Joint Statement on the Use of Surveillance Spyware in the EU and Beyond," Wikimedia, September 4, 2024, https://wikimedia.brussels/a-joint-statement-on-the-use-of-surveillance-spyware-in-the-eu-and-beyond/.

2 Venice Commission, *Report on a rule of law and human rights compliant regulation of spyware*, CDL-AD(2024)043, adopted on 6–7 December 2024 (published in 2025), document available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e.

3 Original title: Spyware.

4 "Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act)," (Official Journal of the European Union, April 17, 2024), available at: https://eur-lex.europa.eu/eli/reg/2024/1083/oj/eng.

5 EDRi, *Spyware and state abuse: The case for an EU-wide ban* (EDRi, June 16, 2025), available at: https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf.

6 The Constitution of the Republic of Serbia, "Official Gazette of RS," no. 98/2006 and 115/2021.

7 The Constitution of the Republic of Serbia, Article 41.

8 The Constitution of the Republic of Serbia, Article 42.

9 The Criminal Procedure Code, "Official Gazette of the Republic of Serbia," no. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – decision of the Supreme Court and 62/2021 – decision of the Administrative Court.

10 The Criminal Procedure Code, Article 162.

11 The Criminal Procedure Code, Article 161.

12 The Criminal Procedure Code, Article 167.

13 The Criminal Procedure Code, Article 168.

14 The Criminal Procedure Code, Article 166.

15 The Criminal Procedure Code, Article 169.

16 The Criminal Procedure Code, Article 170.

17 The Criminal Procedure Code, Article 163.

18 The Criminal Procedure Code, Articles 163 and 84.

19 The Criminal Code, "Official Gazette of the Republic of Serbia," no. 85/2005, 88/2005 – amended, 107/2005 – amended, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 and 94/2024.

20 The Criminal Code, Article 143.

21 The Criminal Code, Article 146.

22 The Criminal Code, Article 298.

23 The Criminal Code, Article 299.

24 The Criminal Code, Article 300.

25 The Criminal Code, Article 301.

26 The Criminal Code, Article 304a.

27 The Draft Law on Amendments to the Criminal Procedure Code, https://ekonsultacije.gov.rs/topicOfDiscussionPage/529/4.

28 The Draft Law on Amendments to the Criminal Code, https://ekonsultacije.gov.rs/topicOfDiscussionPage/528/4.

29 Article 162, paragraph 1, item 2, amendments to the Criminal Procedure Code.

30 Article 112, item 20, amendments to the Criminal Code.

31 Article 163 of the Code of Criminal Procedure.

32 The Law on the Intelligence Agency, "Official Gazette of the Republic of Serbia," no. 42/2002, 111/2009, 65/2014 – decision of the Constitutional Court, 66/2014 and 36/2018.

33 The Law on the Intelligence Agency, Article 13.

34 The Law on the Intelligence Agency, Article 14.

35 The Law on the Intelligence Agency, Articles 15 and 15a.

36 The Law on the Intelligence Agency, Article 15g.

37 The Law on Military Security (VBA) and Military Intelligence Agency (VOA), "Official Gazette of the Republic of Serbia," no. 88/2009, 55/2012 – decision of the Constitutional Court and 17/2013.

38 The Law on Military Security (VBA) and Military Intelligence Agency (VOA), Article 6.

39 The Law on Military Security (VBA) and Military Intelligence Agency (VOA), Article 12.

40 The Law on Military Security (VBA) and Military Intelligence Agency (VOA), Article 13.

41 The Law on Military Security (VBA) and Military Intelligence Agency (VOA), Article 13a.

42 The Law on Electronic Communication, "Official Gazette of the Republic of Serbia," no. 44/2010, 60/2013 – decision of the Constitutional Court, 62/2014, 95/2018 – other law and 35/2023 – other law.

43 The Law on Electronic Communication, Article 126.

44 The Law on Electronic Communication, Article 127, paragraphs 1 and 4.

45 The Law on Electronic Communication, Article 127, paragraphs 2 and 3.

46 The Law on Electronic Communication, Article 129.

47 The Law on Electronic Communication, Article 128.

48 The Rulebook on Requirements for Devices and Software for Lawful Interception of Electronic Communication and Technical Requirements for Fulfilling the Obligation to Retain Data on Electronic Communication, "Official Gazette of RS," 88/2015.

49 The Rulebook on Requirements for Devices and Software for Lawful Interception of Electronic Communication and Technical Requirements for Fulfilling the Obligation to Retain Data on Electronic Communication, Article 1.

50 The Rulebook on Requirements for Devices and Software for Lawful Interception of Electronic Communication and Technical Requirements for Fulfilling the Obligation to Retain Data on Electronic Communication, Article 2, paragraph 1, item 6.

51 The Rulebook on Requirements for Devices and Software for Lawful Interception of Electronic Communication and Technical Requirements for Fulfilling the Obligation to Retain Data on Electronic Communication, Article 26.

52 The Law on Personal Data Protection, "Official Gazette of RS," no. 87/2018.

53 The Law on Personal Data Protection, Article 6, Paragraph 3.

54 The Law on Personal Data Protection, Article 5.

55 The Law on Personal Data Protection, Article 13.

56 The Law on Personal Data Protection, Article 48.

57 The Law on Personal Data Protection, Article 51.

58 The Law on Personal Data Protection, Article 54.

59 The Law on Information Security, "Official Gazette of RS," no. 91/2025.

60 The Law on Information Security, Article 2, paragraph 2, item 13.

61 Venice Commission, *Report on a rule of law and human rights compliant regulation of spyware.*

62 Venice Commission, *Report on a rule of law and human rights compliant regulation of spyware.*

63 Venice Commission, *Report on a rule of law and human rights compliant regulation of spyware.*

64 Available at: "Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists," Amnesty International, December 16, 2024, https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/.

65 More available at: "Serbia: BIRN journalists targeted with Pegasus spyware," Amnesty International, March 27, 2025, https://www.amnesty.org/en/latest/news/2025/03/serbia-birn-journalists-targeted-with-pegasus-spyware/.

66 More available at: NSO (2022), https://www.nsogroup.com/Newses/on-june-21-2022-nso-group-appeared-before-the-eu-parliament-to-speak-on-the-importance-of-the-use-of-the-technology-the-principles-that-guide-our-company-and-to-continue-pushing-for-international-r/.

67 More available at: Aleksa Tešić, "Nova žrtva špijunskog nadzora: student priveden na šest sati, telefon mu hakovan," *Birn.rs*, February 28, 2025, https://birn.rs/student-spijunski-nadzor-hakovan-telefon/.

68 More available at: "Serbia: Civil society threatened by spyware," Amnesty International Security Lab, November 28, 2023, https://securitylab.amnesty.org/latest/2023/11/serbia-civil-society-threatened-by-spyware/.

69 Available at: https://sharefoundation.info/wp-content/uploads/Krivicna-prijava-VTK-Dec-2024.pdf.

70 Available at: https://sharefoundation.info/wp-content/uploads/Zahtev-za-pokretanje-nadzora-Poverenik-Dec-2024.pdf.

71 Available at: https://sharefoundation.info/wp-content/uploads/Zahtev-za-pokretanje-postupka-Zastitnik-gradjana-Dec-2024.pdf.

72 Available at: https://sharefoundation.info/wp-content/uploads/CoE_Urgent-Concerns-Regarding-Use-of-Spyware-in-Serbia-Dec-2024.pdf.

73 Law on Police, "Official Gazette of the Republic of Serbia," No 6/2016, 24/2018 and 87/2018, Article 224.

74 Law on Intelligence Agency, Article 7.

75 National Assembly of the Republic of Serbia, Security Services Control Committee, http://www.parlament.gov.rs/%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B0-%D1%81%D0%BA%D1%83%D0%BF%D1%88%D1%82%D0%B8%D0%BD%D0%B0/%D1%81%D0%B0%D1%81%D1%82%D0%B0%D0%B2/%D1%80%D0%B0%D0%B4%D0%BD%D0%B0-%D1%82%D0%B5%D0%BB%D0%B0/%D0%BE%D0%B4%D0%B1%D0%BE%D1%80%D0%B8.157.13.html.

76 Cellebrite has announced that it is stopping the use of forensic tools in Serbia, more available at: Natalija Jovanović, "Kompanija Cellebrite zaustavlja upotrebu forenzičkih alata u Srbiji nakon izveštaja Amnestyja," *Radio Slobodna Evropa*, February 26, 2025, https://www.slobodnaevropa.org/a/kompanija-cellebrite-upotreba-forenzickih-alata-u-srbiji-nadzor/33328912.html.

77 EDRi, *Spyware and state abuse: the case for an EU-wide ban*, 26.

78 *Szabó and Vissy v. Hungary*, judgment available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160020%22]}.

79 Guide to Article 8, Council of Europe, available at: European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights" (Council of Europe, 2025), 65, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

80 *Weber and Saravia v. Germany*, judgment available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76586%22]}.

81 Venice Commission, *Report on a rule of law and human rights compliant regulation of spyware*, 45.

82 *Weber and Saravia v. Germany*.

83 Venice Commission, *Report on a rule of law and human rights compliant regulation of spyware,* 34.

84 *Goodwin v. United Kingdom*, p. 133, judgment available at: https://www.ucpi.org.uk/wp-content/uploads/2017/11/Goodwin-v-UK-1996-22-EHRR-123.pdf.

85 OHCHR, "Basic Principles on the Role of Lawyers," September 7, 1990, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-role-lawyers.

86 *Z. v. Finland*, available at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.poverenik.rs%2Fimages%2Fstories%2Fpraksazastita%2Fodluke-medjunarodnih-i-stranih-sudova-i-tela%2Flatzvfinland.doc&wdOrigin=BROWSELINK.

87 Venice Commission, *Report on a rule of law and human rights compliant regulation of spyware*, 44.

88 "The European Parliament Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP))" (European Parliament, 2023), available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf.

POLICY PAPER / 1

BCSP Belgrade Centre for Security Policy

SPYWARE

THE NEGATION OF HUMAN RIGHTS UNDER THE PRETEXT OF "SECURITY"

Milica Tošić

Translation:
Nataša Šofranac

This publication was produced with the support of the Norwegian Ministry of Foreign Affairs. Its content is the sole responsibility of the author and does not necessarily reflect the views of the Kingdom of Norway.

DOI: https://doi.org/10.55042/QRFW3664

ISBN-978-86-6237-269-7

January 2026