THE ESTABLISHMENT AND DEVELOPMENT OF A NATIONAL CRIMINAL INTELLIGENCE SYSTEM IN THE REPUBLIC OF SERBIA

Zoran Đurđević, LLD[1]
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Nenad Milić, LLD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Abstract: Efficient countering contemporary forms of crime, especially terrorism, high-tech and organised crime, requires a multi-agency approach and cooperation, both at the national and international level. One of the basic indicators for assessing the quality of cooperation is the exchange of information. The exchange of information overcomes limited resources, and improves the efficiency and cost-efficiency of the evidentiary procedure. The National Criminal Intelligence System is based on the establishment of a Platform for secure electronic communication, exchange of data and information between government authorities, special organisational units of government authorities and institutions, in order to prevent organised crime and other forms of serious crime. The following institutions are participating in the first phase of the establishment of the National Criminal Intelligence System: the Ministry of Interior; Ministry of Justice; Republic Public Prosecutor's Office; Prosecutor's Office for Organised Crime; Office of the National Security Council and Classified Information Protection; Customs Administration; Anti-Corruption Agency; and Tax Administration. The subject of this paper is the analysis of the legal framework, defining of recommendations, establishing which issues need to be legally regulated and which legal acts should be adopted to create the legal conditions necessary for the establishment and development of the NCIS.

Keywords: National Criminal Intelligence System, information exchange, cooperation of government agencies, countering organised crime.

1 zoran.djurdjevic@kpu.edu.rs.

INTRODUCTION

Efficient countering of contemporary forms of crime requires a multi-agency approach – cooperation of all government authorities. Security is not within the exclusive competence of only one government authority; efficient protection of fundamental rights and freedoms of citizens is directly conditioned by the quality of multi-agency cooperation of government authorities within their clearly defined competencies. One of the most important indicators of the quality of cooperation and multi-agency approach is the exchange of information. The exchange of information overcomes limited resources and improves efficiency in combating crime.

Quality cooperation in the information exchange is the basis for threat assessment, detection and proof of crimes, especially the most serious one – organised crime (see more in Đurđević & Radović, 2016). Given the number of exchanged data, it is especially necessary to point out that this fact is clearly visible in the conventions and decisions adopted by the European Union. Among the most important is the 2006 Framework Decision, which simplifies the exchange of information and intelligence between law enforcement authorities (Official Journal of the European Union, L 386/89). In order to regulate the obligations of their government authorities in more detail, individual states have enacted special laws (for example, Croatia: Act on Simplifying the Exchange of Data between Law Enforcement Authorities of the Member States of the European Union, Official Gazette, 56/15). A slightly different law, which, in addition to the exchange of information, regulates the manner of organisation of criminal intelligence activities, which is the topic of this paper, was also passed by Lithuania (Law on State Secrets and Official Secrets, 13/06/2017 – No. XIII-437).

At the international level, the police of the Republic of Serbia exchanges a large amount of data (INTERPOL, EUROPOL, SELEC, but also bilaterally), respecting the standards set by the Swedish Initiative, including the principle of "equivalent approach". A secure communication link via the EUROPOL's Secure Information Exchange Network Application (SIENA) was established in 2012, and an operational agreement with EUROPOL was signed in 2014. From June 1, 2014 until February 22, 2016, a total of 7,210 messages were exchanged via the SIENA application (Action Plan for Chapter 24 – Justice, Freedom, Security, p. 124).

The subject of the authors' analysis is the National Criminal Intelligence System of the Republic of Serbia (hereinafter: NCIS), that is, the exchange of information aimed at improving the efficiency in combating organised crime. In order to ensure the exchange of information relevant for combating crime, it is necessary to define a coherent and methodologically harmonised approach, through improving and strengthening the information exchange capacities, the concretisation of which would involve harmonisation of legal regulations governing standards of information management and exchange between government authorities. The said task is in line with the recommendation of the European Commission and based on it planned activity set out in the Action Plan for Chapter 24, subchapter Organised Crime (Activity 6.2.2).

The National Criminal Intelligence System represents the second phase of the reorganisation of work and change in the philosophy of procedure based on intelligence information in the Ministry of Interior of the Republic of Serbia. The first phase was the implementation of the Intelligence-Led Policing Model in the work of the Ministry of Interior (see more in: MoI, 2016; Đurđević & Leštanin, 2017; Đurđević & Vuković, 2018). The establishment of the NCIS takes place in two interconnected, mutually conditioned directions: the creation of technical conditions for the exchange of data and the adoption of legal acts that will regulate this exchange. The paper will primarily focus on the analysis

of the legal framework necessary for the establishment and development of the NCIS in the Republic of Serbia.

The following institutions are participating in the establishment of the NCIS: the Ministry of Interior; Ministry of Justice; Republic Public Prosecutor's Office; Prosecutor's Office for Organised Crime; Office of the National Security Council and Classified Information Protection; Customs Administration; Anti-Corruption Agency; and Tax Administration.

METHODOLOGICAL FRAMEWORK OF THE ANALYSIS

In order to draw conclusions and define recommendations on how to create the necessary legal conditions for the implementation of the NCIS, the subject of the analysis were:

1. Legal acts governing cooperation, primarily the exchange of data, between government authorities in the fight against crime.
2. Legal acts governing the collection, processing, protection, keeping, exchange and use of data.

Special attention was paid to the legal basis for record keeping and standards for working with data:

- Data systematisation criteria; protected data, classified data;
- Data security threat assessment;
- Protection measures (special zone – a place where the records are kept, construction safeguards, physical safeguards, technical safeguards, measures to protect the information and telecommunication systems, crypto-protection);
- Legal regulation of job positions that can have access to data of different classification levels for each record;
- Person responsible for information management;
- Legally regulated system of data management supervision;
- Internal control plan for handling classified data; and
- Records of decisions on the classification level security clearances (exists/doesn't exist, person responsible for the records)

The aim of the analysis was to define, based on the applicable law regulating the exchange of data between government agencies, the following:

- Recommendations on general legal acts that need to be adopted in order to create legal conditions for the establishment and operation of the NCIS.
- Recommendations on which legal and practical standards in data management must be achieved by each NCIS participant.

To identify organisational factors relevant for the implementation and development of the NCIS, a SWOT analysis was carried out.

APPLICABLE LAW ANALYSIS

The subject of the analysis of the legal framework for the establishment and development of the NCIS was focused on two issues: the analysis of the applicable law governing the exchange of data between government authorities and institutions and the analysis of the necessary legal framework for the exchange of data within the NCIS.

In the applicable law of the Republic of Serbia, there are a large number of general legal acts that in a certain way, in accordance with the purpose of their adoption, regulate cooperation, exchange and management of data that may be relevant for proving organised and serious crime. The legal basis for cooperation between government authorities is defined by the Law on State Administration (Article 64), in accordance with which state administration authorities are obliged to cooperate in all joint issues as well as to provide each other with data and information necessary for their work. State administration authorities may also establish joint bodies and project groups for the purpose of executing tasks whose nature requires the participation of several state administration authorities, which by its nature and essence is the NCIS.

Assistance and cooperation in combating the most serious forms of crime is regulated by the Criminal Procedure Code (Official Gazette of the Republic of Serbia, Nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 and 35/2019) and the Law on Organisation and Jurisdiction of Government Authorities in the Suppression of Organised Crime, Terrorism and Corruption (Nos. 94/2016 and 87/2018).

The duty to provide assistance to participants in criminal proceedings is provided by the Criminal Procedure Code (Article 19), according to which all government authorities are obliged to provide the necessary assistance to the public prosecutor, court or other authority conducting proceedings, as well as to the defendant and his/her defence attorney at their request for the purpose of collecting evidence.

The Law on Organisation and Jurisdiction of Government Authorities in the Suppression of Organised Crime, Terrorism and Corruption raises the cooperation of government authorities to a higher level, by creating the possibility for government authorities to appoint their liaison officer to establish cooperation and more efficiently deliver data received from these authorities and organisations to the Prosecutor's Office for Organised Crime and special departments of higher public prosecutor's offices for the suppression of corruption, for the purpose of criminal prosecution for criminal offenses provided by this Law (Article 20). Task forces may also be formed within the Prosecutor's Office for Organised Crime and special departments of higher public prosecutor's offices for the suppression of corruption, with the aim of detecting and prosecuting crimes they deal with (Article 21).

All legal acts, laws and other general acts important for the cooperation and data management have been systemised into several groups:

- Laws and other general legal acts governing the cooperation of government authorities, especially in combating organised crime.[2]
- Laws and other general legal acts governing the protection of classified data and access to data.[3]

2 The following were analysed: the Criminal Procedure Code; Law on Organisation and Jurisdiction of Government Authorities in the Suppression of Organised Crime, Terrorism and Corruption; and the Law on State Administration.

3 The following were analysed: the Data Secrecy Law; Law on Information Security; Law on Personal Data Protection; Law on the Protection of Trade Secrets; and the Law on Free Access to Information of Public Importance.

- Laws related to data protection during the course of work, undertaking actions within the competence of government authorities and agencies.[4]
- Laws containing penal provisions for actions incriminated as criminal offences and/or misdemeanours for data confidentiality violations.[5]

The first step towards the establishment of the NCIS was made in the Law on Police (Official Gazette of the Republic of Serbia, Nos. 6/2016, 24/2018 and 87/2018). Article 34a provides for the establishment of the Platform for secure electronic communication, exchange of data and information between government authorities, special organisational units of government authorities and institutions, in order to prevent organised crime and other forms of serious crime, within the special information and communication system of the Ministry. The Platform represents a technical instrument with the help of which the data will be exchanged within the NCIS. The second step, which actually also represents the beginning of the materialisation of this idea, is the signing of the Agreement on Cooperation on Establishing and Developing a National Criminal Intelligence System (September 2019). The Agreement defines the subject, goal, forms of cooperation, and authorities responsible for the establishment and development of the NCIS. The signatories agreed to establish and develop the NCIS, in order to build a system of continuous electronic exchange of data and information, as well as coordination to strengthen a proactive approach in combating organised crime and other forms of serious crime (Agreement, Article 3). For the establishment of the NCIS, that is, the realisation of the tasks provided for in the Agreement, a Permanent Working Body and an Interdepartmental Working Group were established. The Permanent Working Body adopted the Rules of Procedure and several conclusions related to the first steps aimed at establishing the NCIS. The Interdepartmental Working Group is an operational body which, in line with the conclusions of the Permanent Working Body, undertakes the necessary activities in order to establish, develop and implement the NCIS.

To objectively understand the purpose and place of the NCIS in the security system, it is necessary to clearly define what the NCIS is and what the difference between the NCIS and the Security Intelligence System is.

The security-intelligence system of the Republic of Serbia is legally regulated by the Law on the Bases Regulating the Security Services Organisations (Official Gazette of the Republic of Serbia, Nos. 116/2007 and 72/2012). Its goal is to direct, harmonise and supervise the security services work. The Ministry of Interior and other participants in the first phase of the NCIS do not belong to the security services and their goal is to improve the efficiency in preventing and fighting organised crime and other forms of serious crime. Analogously to the above stated, *the National Criminal Intelligence System* can be most simply understood as a system of government authorities and institutions whose goal is to improve cooperation and institutional capacity in combating organised and other forms of serious crime through data exchange.

4 The following were analysed: the Criminal Procedure Code; Law on Organisation and Jurisdiction of Government Authorities in the Suppression of Organised Crime, Terrorism and Corruption; Law on the Bases Regulating the Security Services Organisations in the Republic of Serbia; Law on Police; Law on Records and Data Processing in the Field of Internal Affairs; Law on Public Prosecutor's Office; Law on Civil Servants; Law on Tax Procedure and Tax Administration; Law on Customs Service; Customs Law; Law on the Prevention of Money Laundering and Terrorist Financing; Law on the Anti-Corruption Agency; Law on Banks; Law on the Security Information Agency; Law on the Military Security Agency and the Military Intelligence Agency; and the Law on the Serbian Army.

5 The Criminal Code: Unauthorised Disclosure of Secret (Article 140), Disclosure of Business Secret (Article 240), Disclosure of State Secret (Article 316), Disclosure of Official Secret (Article 369), Disclosure of Military Secret (Article 415); Data Secrecy Law (Articles 98, 99 and 100); Law on Personal Data Protection (Article 57); Law on Information Security (Articles 30 and 31); Law on the Protection of Trade Secrets (Corporate Offence, Article 19).

DATA EXCHANGE STANDARDS

For the establishment of the NCIS, it is necessary to adopt common standards for data handling, protection, access and exchange.

The defined standards for access to specific data must be respected by all officials of all government authorities who wish to gain access to the database in which the data are stored. It is certainly necessary to pay special attention to respecting the standards in the exchange of the classified and personal data. The law regulating the system of the classification and protection of classified data of interest for the national security and public safety, defence, internal and foreign affairs of the Republic of Serbia, protection of foreign classified data, access to classified data and their declassification is the Data Secrecy Law (Official Gazette of the Republic of Serbia, No. 104/2009).

A special subject of the analysis were the standards that must be respected in the NCIS's work, which are defined by this law and relate to: ***protection*** of data confidentiality (protection criteria, protection measures: general and special, obligations of the data handlers, storage, transfer and submission of classified data), ***access*** to classified data, procedure for providing security clearance, that is, permits ***for access*** to classified data.

These standards are the basis for defining the conditions that must be met for the exchange of data between the members of the NCIS. In order to exchange data, the party taking over the data must respect the same standards in their work as the data owner. In particular, it should be emphasised that only a person who has the appropriate security clearance in relation to the classification level with which the data (which is the subject of exchange) is marked, can have access to it.

Analogously to the above mentioned related to the establishment of the NCIS, it is necessary that everyone consistently apply the provisions of the Data Secrecy Law, in particular, all participants in the NCIS must have ***an authorised person to classify the data*** (Article 9) and adopt standards for classifying and marking the level of secrecy.

To determine the classification level, it is necessary ***to assess the possible damage*** that the disclosure of information may have to the interests of the Republic of Serbia.

Criteria for assigning the "TOP SECRET" and "SECRET" classification levels are determined by the Government, with previously obtained opinion from the National Security Council, while criteria for determining the "CONFIDENTIAL" and "RESTRICTED" classification levels are determined by the Government, at the proposal of the competent minister or head of a public government authority. The Government of the Republic of Serbia has passed the Decree on Detailed Criteria for Assigning the "TOP SECRET" and "SECRET" Classification Levels (Official Gazette of the Republic of Serbia, No. 46/13).

The authorised person of the public authority, in accordance with the Data Secrecy Law, and on the basis of the criteria referred to in Articles 3 and 4 of the Decree on Detailed Criteria for Assigning the "TOP SECRET" and "SECRET" Classification Levels, makes a decision on determining the data classification level in a public authority, with preliminary assessments of possible damage to the interest of the Republic of Serbia. In accordance with Article 14, paragraph 4 of the Data Secrecy Law, the Government of the Republic of Serbia has passed a series of regulations on detailed criteria for determining the "CONFIDENTIAL" and "RESTRICTED" classification levels in the work of specific government authorities and institutions. These regulations are similar in terms of their structure, with certain adjustments when it comes to the criteria for determining the "CONFIDENTIAL" and "RE-

STRICTED" classification levels. However, it can be said that the criteria for determining the classification level are overly general and difficult to scale. The decision on determining the data classification level, with a preliminary assessment of possible damage to the interest of the Republic of Serbia, that is, possible damage to the work and performance of tasks and duties of public authorities, is made by the person authorised to perform data classification. The Data Secrecy Law, as well as the regulations, do not regulate in detail who shall be the authorised persons of the public authority who shall determine the level of data secrecy. Specifically, in relation to three possible solutions – to be determined by law, by a regulation adopted on the basis of law, or to be authorised in writing by the head of a public authority – the third option is applied in practice: the person authorised to perform the data classification is authorised in writing by a head of a public authority.

Protection Measures

In accordance with the Data Secrecy Law, adequate data protection measures (general and special protection measures) must be applied in the exchange of data, in relation to the classification level, the nature of the document containing the classified data and the threat assessment. Since the data will be exchanged electronically, it is necessary to pay special attention to the provisions of the Law on Information Security (Official Gazette of the Republic of Serbia, Nos. 6/2016 and 94/2017). The law provides for measures to protect against security risks in information and communication systems, the liability of legal persons in the management and use of information and communication systems, competent authorities for the implementation of protection measures, coordination between protection stakeholders and monitoring the proper application of prescribed protection measures.

Access to Data

It still has not been precisely regulated who can have access to specific data of a certain classification level, that is, which employee, in relation to the type of work and place in the hierarchy of an organisation, should have a security clearance to access data.

The circle of persons who can access classified data without a security clearance and security clearance is determined by the Data Secrecy Law. The President of the National Assembly, President of the Republic and the Prime Minister have access to classified data and can use data and documents of any classification level without a security clearance. Likewise, government authorities appointed by the National Assembly, heads of government authorities appointed by the National Assembly, judges of the Constitutional Court and judges, are authorised to access data of any classification level that they need to perform tasks within their competence, without security clearance. However, there are limitations to this rule when it comes to access to data classified as "SECRET" and "TOP SECRET" (Data Secrecy Law, Article 38, paragraph 2).

Any other person, in relation to the security clearance, can access the data for which the security clearance was issued. Keeping records on persons who are allowed access to classified information is regulated by *the Decree on the Content, Form and Manner of Keeping Records of Access to Classified Information* (Official Gazette of the Republic of Serbia, No. 89/2010).

When it comes to the security clearance issuing procedure, the form of the basic and special security questionnaire for individuals and legal persons is prescribed by *the Decree on Forms of Security Ques-*

tionnaires (Official Gazette of the Republic of Serbia, No. 30/2010). The content, form and manner of providing a security clearance for access to classified information is prescribed by *the Decree on the Content, Form and Manner of Providing Security Clearances for Access to Classified Information* (Official Gazette of the Republic of Serbia, No. 54/2010).

Data Exchange

Classified data may be delivered to another public authority under *a written authorisation issued by the authorised person of the public authority* who marked the data as classified, unless otherwise provided by a special law (Data Secrecy Law, Article 45). Classified data received from a public authority may not be delivered to another user without the consent of the authority which designated the data as classified, *unless otherwise provided by a special law*. Persons who perform tasks in a public authority to which classified data have been delivered *are obliged to respect the security classification markings* and to take the protection measure determined for that classification level.

An authorised person may submit classified data to another legal or natural person, who provide services to a public authority on the basis of a contractual relationship, only in specific situations defined in the Data Secrecy Law (Article 42).

Personal Data Protection

The Constitution of the Republic of Serbia (Article 42) guarantees the protection of personal data. In accordance with the Constitution, collecting, keeping, processing and using of personal data are regulated by law. Records containing personal data cannot be regulated by a bylaw.

Personal data may be used and forwarded further only to the extent not contrary to the purpose for which they were collected, except for the purposes of conducting criminal proceedings or protecting the security of the Republic of Serbia, in a manner stipulated by law.

When protecting personal data, the principle of limited purpose and the principle of security, as well as the right of access, must be especially respected. Above all, it is necessary to apply the measures stipulated in Article 51 of the Law on Personal Data Protection (Official Gazette of the Republic of Serbia, No. 87/2018).

Supervisory Measures over the Handling of Classified Information

The Decree on Special Measures for the Supervision of Handling Classified Information (Official Gazette of the Republic of Serbia, No. 90/2011) stipulates the obligation to take special measures of supervision over the handling of classified information in a public authority.

Special supervisory measures include direct inspection, appropriate checks and reviews of submitted reports related to the implementation of all measures for the protection of classified information, or one or certain measures for the protection of classified information, and are carried out through internal control.

CONCLUSIONS ON THE FULFILMENT OF STANDARDS FOR THE NCIS' WORK

Based on the conducted analyses of the applicable law and implemented data management standards for the establishment of the NCIS, the following conclusions can be drawn:

1. In the Republic of Serbia, there is a legal framework that to a certain extent can be used for the establishment and operation of the NCIS. However, for quality work and exchange of information, it is necessary to pass a special law and a set of bylaws for a more specific elaboration of legal provisions of the law which would be passed.
2. The government authorities and institutions that will make up the NCIS are at different levels of implementation of data management standards. It is necessary to define and implement data exchange standards in the NCIS, including records on exchanged data.
3. The data exchanges currently being implemented between the government authorities and institutions that make up the NCIS should be placed within the framework of the NCIS.
4. For the successful implementation of the NCIS, it is necessary to perform an analysis of the professional potential of each government authority and of adequate security clearances for access to data that will be exchanged.

It is extremely important to identify all the factors on which successful establishment of the NCIS may depend. Awareness of the potentially great benefit for the work of each authority – for the efficient detection and proof of organised crime and other serious crimes – is a factor on which the work of the NCIS directly depends. Lack of awareness of the need to improve data exchange directly leads to a lower degree of efficiency.

In order to systematically approach the creation of conditions necessary for the functioning of the NCIS, it is necessary to focus on two groups of activities.

The first group of activities includes measures to improve the work, which are the result of the evaluation of the achieved standards defined in the Data Secrecy Law. The recommendations should be independently considered and implemented by each member of the NCIS.

All members of the NCIS need to meet the data management standards, that is, those members that have not met them yet, and above all to:

- Adopt a legal act, preferably a law that would regulate the keeping of records related to their competence (if the records contain personal data, the law is necessary).
- Designate an authorised person to mark the classification level, procedure and assessment methods. It is necessary to define more detailed criteria for the selection of an authorised person to classify data; the best would be in relation to the person's functional position in the organisation, which should be precisely defined in the regulation on internal organisation and classification of job positions.
- Designate a classified data controller;
- In relation to the type of work and a place in the organisation's hierarchy, define who can access which data, which should be precisely defined in the regulation on internal organisation and classification of job positions.
- Establish records of decisions on the security clearances for "CONFIDENTIAL", "SECRET", "TOP SECRET" classification levels, and records of statements for access to classified information classified as "RESTRICTED" for persons who perform a function or are employed in a public authority, and for persons who perform specific tasks in accordance with the law governing the classified information.

The second group of activities is aimed at creating specific conditions for technical connection to the platform and developing a legal framework for the work of the NCIS. The recommendations on how to achieve these standards should be adopted and implemented by the Permanent Working Body for Monitoring the Implementation of the Agreement on Cooperation on Establishing and Developing a National Criminal Intelligence System.

Given the fact that cooperation and exchange of data by government authorities and institutions is regulated by various legal acts in the hierarchy of legal acts, the exchange of information within the NCIS, as already pointed out, must be regulated by a special law. Adoption of a lower-level legal act than the law would require a long period of time needed for the harmonisation of the legal framework for the establishment of the NCIS by the government authorities that will make it. The only expedient and legally logical solution is the adoption of a special law: the Law on the National Criminal Intelligence System of the Republic of Serbia. In order to concretise the legal provisions and fully regulate the legal framework, it is necessary to adopt regulations, rulebooks and other legal acts that will regulate issues related to: the manner of data exchange; registering access to the NCIS Platform; records of data subject to exchange; security threat assessment and protection measures; supervision and work of persons authorised to supervise the exchange of data within the NCIS.

All provisions of the Law on Information Security must be observed when establishing the NCIS, and among other things, it is necessary to: designate an ICT system operator (MoI – Sector for Analytics, Telecommunication and Information Technologies – SATIT) and each signatory its authorised person for security management; choose a system of work ("non-selective"; "selective"; "multi-level"); form a body for coordination of information security protection measures; define obligations and responsibilities between the operator and other members of the NCIS; define the procedure for notifying the competent authority (operator, National CERT) of an incident, loss, theft, damage, destruction or unauthorised disclosure of classified information and foreign classified information, as well as of violation of the right to personal data protection. What is particularly important is that every access to the information and communication system is recorded. In order for the mentioned activities to be realised, it is necessary to adopt the Rulebook on the Security Threats Assessment and Defining the NCIS Protection Measures.

In order to coordinate the prevention and protection against security risks in the ICT system, it is necessary to keep in mind the cooperation with the National CERT (Regulatory Agency for Electronic Communications and Postal Services) and the Centre for the Prevention of Security Risks in ICT Systems in the republic authorities (CERT of republic authorities).

For the successful development of the NCIS, it is necessary to define a development strategy and implementation plan that will include: involvement of other government authorities and institutions; exchange of classified information and documents (especially orders on taking special evidentiary actions), continuous technical improvement of the platform's work and protection measures; promotion and improvement of professional capacities of law enforcement agencies.

In order to improve the level of efficiency in combating crime, especially organised crime, terrorism and corruption, it is necessary to strengthen joint analytical capacities. Likewise, it is necessary to continuously work on the education of all the NCIS users, with the organisation of special trainings necessary for risk analysis, and data protection and exchange. It is also necessary to envisage ways to exchange experiences and identify possible problems.

The Permanent Working Body is an organisational form necessary for the beginning of the work of the NCIS, which will hardly support the development component. Analogously, it is necessary to form a Data Exchange Centre or an organisational unit of another form with the same function, with perma-

nent employees. The centre as a form of organisation can be the subject of analysis, and thus change, depending on the selected strategic direction of development and current opportunities.

REFERENCES

1. Council Framework Decision 2006/960/JHA, Official Journal of the European Union, L 386/89.
2. Djurdjevic, Z. & Lestanin, B. (2017). Intelligence-Led Policing in the Ministry of Interior of the Republic of Serbia. Thematic conference proceedings of international significance "Archibald Reiss Days", Academy of Criminalistic and Police Studies, Belgrade, Vol. 3, pp. 3–16.
3. Djurdjevic, Z. & Vukovic, S. (2018). Current Situation and Perspectives of Intelligence-Led Policing Model in the Republic Serbia. Conference: Criminal Justice and Security in Central and Eastern Europe – From Common Sense to Evidence-Based Policy-Making, University of Maribor, Faculty of Criminal Justice and Security, pp. 158–167.
4. Министарство унутрашњих послова Републике Србије (2016). Полицијско-обавештајни модел: приручник. Београд: Министарство унутрашњих послова Републике Србије. [Ministry of Interior of the Republic of Serbia (2016). Intelligence-Led Policing: Handbook. Belgrade: Ministry of Interior of the Republic of Serbia]
5. Radovic, N. & Djurdjevic, Z. (2016). European Union's Information Exchange Legal Framework – A Prerequisite for Successful Co-Operation in Fighting Organized Crime. *Journal of Criminalistics and Law*, 3/2016, pp. 95–117.
6. Ratcliffe, J. H. (2016). Intelligence-Led Policing (2nd ed.). New York: Routledge.
7. Влада Републике Србије (2016). Акциони план за поглавље 24 – Правда, слобода, безбедност, Београд: Влада Републике Србије. [Government of the Republic of Serbia (2006). Action Plan for the Chapter 24 – Justice, Freedom, Security, Belgrade: Government of the Republic of Serbia]
8. Law on State Secrets and Official Secrets of the Republic of Lithuania, Official Gazette of the Republic of Lithuania, 13/06/ 2017 – No. XIII-437.
9. Устав Републике Србије, Службени гласник РС, бр. 98/2006. [Constitution of the Republic of Serbia, Official Gazette of the Republic of Serbia, No. 98/2006]
10. Уредба о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА" и „СТРОГО ПОВЕРЉИВО", Службени гласник РС, бр. 46/13. [Decree on Detailed Criteria for Assigning the "TOP SECRET" and "SECRET" Classification Levels, Official Gazette of the Republic of Serbia, No. 46/13]
11. Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима, Службени гласник РС, бр. 89/2010. [Decree on the Content, Form and Manner of Keeping Records of Access to Classified Information, Official Gazette of the Republic of Serbia, No. 89/2010]
12. Уредба о обрасцима безбедносних упитника, Службени гласник РС, бр. 30/2010. [Decree on Forms of Security Questionnaires, Official Gazette of the Republic of Serbia, No. 30/2010]
13. Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима, Службени гласник РС, бр. 54/2010. [Decree on the Content, Form and Manner of Providing Security Clearances for Access to Classified Information, Official Gazette of the Republic of Serbia, No. 54/2010]

14. Уредба о посебним мерама надзора над поступањем са тајним подацима, Службени гласник РС, бр. 90/2011. [The Decree on Special Measures for the Supervision of Handling Classified Information, Official Gazette of the Republic of Serbia, No. 90/2011]
15. Zakon o pojednostavljenju razmjene podataka između tijela država članica europske unije nadležnih za provedbu zakona Republike Hrvatske, Narodne novine RH, no. 56/15. [Act on Simplifying the Exchange of Data between Law Enforcement Authorities of the Member States of the European Union, Official Gazette of the Republic of Croatia, No. 56/15]
16. Закон о државној управи, Службени гласник РС, бр. 79/2005, 101/2007, 95/2010, 99/2014, 47/2018 и 30/2018. [Law on State Administration, Official Gazette of the Republic of Serbia, Nos. 79/2005, 101/2007, 95/2010, 99/2014, 47/2018 and 30/2018]
17. Законик о кривичном поступку, Службени гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 и 35/2019. [Criminal Procedure Code, Official Gazette of the Republic of Serbia, Nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014 and 35/2019]
18. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције, Службени гласник РС, бр. 94/2016 и 87/2018. [Law on Organisation and Jurisdiction of Government Authorities in the Suppression of Organised Crime, Terrorism and Corruption, Official Gazette of the Republic of Serbia, Nos. 94/2016 and 87/2018]
19. Закон о полицији, Службени гласник РС, бр. 6/2016, 24/2018 и 87/2018. [Law on Police, Official Gazette of the Republic of Serbia, Nos. 6/2016, 24/2018 and 87/2018]
20. Закон о основама уређења служби безбедности, Службени гласник РС, бр. 116/2007 и 72/2012. [Law on the Bases Regulating the Security Services Organisations, Official Gazette of the Republic of Serbia, Nos. 116/2007 and 72/2012]
21. Закон о тајности података, Службени гласник РС, бр. 104/2009. [Data Secrecy Law, Official Gazette of the Republic of Serbia, No. 104/2009]
22. Закон о информационој безбедности, Службени гласник РС, бр. 6/2016 и 94/2017. [Law on Information Security, Official Gazette of the Republic of Serbia, Nos. 6/2016 and 94/2017]
23. Закон о заштити података о личности, Службени гласник РС, бр. 87/2018. [Law on Personal Data Protection, Official Gazette of the Republic of Serbia, No. 87/2018]