

UDK: 355.40 : 343.14 (497.5)
343.14 : 342.721 (497.5)
Review paper

Matko Pajčić, Associate Professor

Faculty of Law, University of Split
E-mail: mpajcic@pravst.hr
ORCID ID: 0000-0003-0657-1245

Zvonimir Tomičić, Associate Professor

Faculty of Law, University of J. J. Strossmayer in Osijek
E-mail: tomicic.zvonimir@pravos.hr
ORCID ID: 0000-0001-6159-6475

Antonio Katavić, Univ. Spec. Iur., PhD Student

Faculty of Law, University of Zagreb
E-mail: antonio.katavic@yahoo.com

POSSIBILITIES AND PITFALLS OF USING INTELLIGENCE DATA AS EVIDENCE IN CROATIAN CRIMINAL PROCEEDINGS

ABSTRACT

In today's world, the reactive approach of law enforcement agencies often cannot fully respond to the challenges posed by certain forms of crime, especially (but not exclusively) those that are narratively committed in a covert manner and that cannot be investigated and prosecuted using conventional criminal methods. Therefore, there is a need for increasingly proactive approaches by law enforcement agencies when solving conceptually complex crimes. Sometimes there may also be a need to use intelligence information, and in this sense, the information and evidence collected by security intelligence agencies in their covert work in the performance of their duties are often extremely valuable. This paper will primarily use comparative and teleological methods to investigate possible legal prerequisites for the lawful use of evidence collected by security intelligence agencies in their work, as well as possible restrictions on the use of such evidence in criminal prosecution. Special attention will be given to the fairness of the use of such evidence in criminal proceedings, as well as possible violations of the right to protection of private and family life, all in accordance with the fundamental postulates of the rule of law. If necessary, de lege ferenda proposals will be presented for possible future changes to the normative framework for the Republic of Croatia.

Keywords: *intelligence service, intelligence data, criminal procedure, evidence admissibility*

1. INTRODUCTION

The work of intelligence agencies at first glance does not have a close relationship with criminal and criminal procedural law. Such a conclusion could be derived from normative rules regulating intelligence agencies on the one hand, and criminal procedure on the other hand. It is evident that the Croatian police and public prosecution service have a primary task to investigate criminal offence, respectively to undertake actions in the event of a criminal offence, according to the Criminal Procedure Act,¹ The Police Duties and Powers Act,² Rulebook on the manner of acting of police officers.³ They collect data that can be relevant to the determination of the criminal offence and the identity of the perpetrator. The task of the police and public prosecutor's office is different from the task of the intelligence agencies namely because they act on after the crime has already been committed. They act according to the principle of *ex officio* preliminary investigation (police) and principle of legality of prosecution (public prosecution service) that require from those organisations that they undertake all prescribed acts in the case of the suspicion of the criminal offence.⁴

Intelligence agencies on the other hand have a primary goal of the long term tracking and collecting data on the threats to the national security. As Badžim nicely described, the intelligence agencies process security threats through criminological-phenomenological approach and the wider national-security context. They are additionally directed to the content which are prior to the commission of the criminal offence and on the content which form the context of the generation of the criminal offence.⁵

¹ Criminal Procedure Act (Croatian: Zakon o kaznenom postupku) Official Gazette, No. 152/2008, 76/2009, 80/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017, 126/2019, 126/2019, 80/2022, 36/2024 (hereinafter: CPA).

² The Police Duties and Powers Act (Croatian; Zakon o policijskim poslovima i ovlastima) Official Gazette No. 76/2009, 92/2014, 70/2019 (hereinafter: Police Act).

³ Rulebook on the manner of acting of police officers (Croatian: Pravilnik o načinu postupanja policijskih službenika), Official Gazette No. 20/2022, 37/2023, 114/2023 (hereinafter: Police Rulebook).

⁴ The principle of legality of criminal prosecution (mandatory criminal prosecution) is applied as a rule in the Republic of Croatia, while the principle of opportunity of criminal prosecution (prosecutorial discretion) is an exception that is applied in individual, precisely prescribed cases by law. Article 2 (3) of the CPA; see also in: Krapac D., *Kazneno procesno pravo, Prva knjiga: institucije*, Narodne Novine, Zagreb, 2015, p. 101. The goal of police is to prevent the criminal offence and in the case of its commitment to carry the criminal investigation on the *ex post facto* basis. Malnar D., Sigurnosno obavještajne studije, Jesenski i Turk, 2024., p. 23-24.

⁵ Badžim J., *Obavještajna državna tijela i kriminalitet*, Split, 2014., p. 234.

Furthermore, the intelligence agencies are directed to collecting information, while the police led intelligence is directed to collecting evidence in the sense of immediate conversion of such information to the evidence admissible in criminal procedure.⁶ Therefore it can be concluded that intelligence agencies can easier collect information about criminal offences because they can recognize possible environmental conditions which can indicate the possible development of criminal offence and gather valuable evidence from its creation stage. As Badžim wrote, intelligence agencies from the basis of its wider knowledge of the criminological and security context and with the help of inductive/deductive method can conclude and make connections of the interconnection between for example criminal offence of forgery of documents and terrorism, which can contribute to the better qualification of the criminal offence.⁷ Because of limitations that traditional criminal investigation bodies face, some authors concluded "that the traditional approaches to address criminality and which are reflected in the Criminal Law, are almost exhausted and overcome in the context of new security challenges (international organized crime, terrorism, cybercrime, etc.)."⁸

Regardless of the above mentioned, intelligence agencies frequently get in touch with criminal offences in the execution of their authorities since they are competent to investigate security threats constituting very often some criminal offences (e.g. terrorism, organised and economic crime, extremism, espionage from other states, organisations and individuals, jeopardizing the safety of protected persons, objects and spaces, unauthorized access to protected information systems/cyberattacks, disclosure of classified information and other security threats). All mentioned activities contain large number of criminal offences, therefore the connection of intelligence agencies with criminal law is more than evident. Intelligence agencies are obliged to notify State Attorney's Office in the case when the collected data indicate that the criminal offence (for which the prosecution is made on the *ex officio* basis) is about to be committed or is already committed.⁹ That notification can exceptionally contain data on the method of data collection. Furthermore, directors of intelligence agencies are authorized to seek the State Attorney to postpone further criminal investigation if

⁶ Potparić D., Veić P., *Uporaba proaktivne kriminalističke obavještajne djelatnosti u borbi protiv teških kaznenih djela i organiziranog kriminaliteta*, Policija i sigurnost, Vol 29., No. 4, Zagreb, 2020., p. 359.

⁷ Badžim, J., *op.cit.*, note 5, p. 313.

⁸ Vaško, A., *Intelligence information within criminal proceedings*, DANUBE: Law, Economics and Social Issues Review, ISSN 1804-8285, De Gruyter, Warsaw, Vol. 10, Iss. 3, 2019, p. 280.

⁹ Act on the Security-Intelligence System of the Republic of Croatia, (Croatian: Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske), Official Gazette, No. 79/2006, 105/2006 (hereinafter: SIS Act) Art. 56 (1).

it's continuation would jeopardize execution of tasks of intelligence agencies or it's sources of information.¹⁰

Therefore, the most important question is whether information collected by intelligence agencies can be used as evidence in criminal proceedings. That is very complex question, definitely not researched enough in criminal procedure law science. Therefore, we will try to shed light on this issue below.

The topic of the paper is analysis of present legal provisions in Croatian legal system. Because of the limited scope of the paper, we will present only very limited comparative analysis (Netherland and United Kingdom). A more comprehensive proposals *de lege ferenda* will be the subject of another paper, preceded by an analysis of the practice of the European Court of Human Rights and broader comparative national legal systems. We pose two hypotheses that we will prove in this paper: 1) Due to their organization, specialized multidisciplinary knowledge, and broader information gathering capabilities, intelligence services are able to collect a lot of evidence about the commission of a criminal offense that is very difficult to collect by criminal prosecution bodies, and therefore the possibility of using this information would significantly contribute to the effectiveness of criminal prosecution for certain types of criminal offenses. 2) The legislative framework in Croatia is inadequate to fully use the potential benefits of intelligence data.

2. DIFFERENT SORTS OF INTELLIGENCE MEASURES AND INTELLIGENCE INFORMATION AS POSSIBLE EVIDENCE OF SIGNIFICANCE TO THE CRIMINAL PROCEEDINGS

2.1. Various measures that intelligence services use to gather information

Intelligence agencies use a wide range of intelligence disciplines for data collection, e.g., OSINT, HUMINT, SIGINT, MASINT, IMINT, FININT, GEOINT¹¹. Intelligence agencies are authorized according to article 33 of the SIS

¹⁰ SIS Act Art. 56 (3).

¹¹ OSINT means an intelligence discipline of data gathering from open sources such as: public media, social networks, internet blogs, public reports, commercial data. HUMINT means an intelligence discipline of data gathering from persons such as: informers, associates or intelligence agents, while SIGINT shortly means an intelligence discipline of data gathering from the intercepted communications or signals in are, for that and other above-mentioned disciplines. Furthermore MASINT means an intelligence discipline which collects and analyzes measurable data (e.g. optical and acoustic measurements).

Act to carry on the clandestine operation measures if the data cannot be gathered in other way or if the gathering of data would be disproportionately difficult. Intelligence agencies shall apply measure which is less intrusive to protected constitutional rights. Clandestine operation measures are almost identical with its content to the special evidentiary actions from the article 332 of the CPA. Some clandestine operation measures (clandestine oversight of telecommunication traffic data, clandestine oversight of location of data subject, clandestine oversight of international telecommunication connections, clandestine surveillance and observation with photo recording of data subjects in open/public area, and clandestine repurchase of documents and items) can be done with the approval of director of intelligence agencies while other more intrusive clandestine operations (clandestine oversight of the content of communication, clandestine oversight of postal and other packages, clandestine oversight and technical recording closed areas/interior, clandestine oversight and observation with audio recording in open areas/public spaces) can as a rule be applied with the warrant of judge from the Supreme Court of Croatia. The main difference from special evidentiary measures from the CPA is that the proposition for issuing the warrant for clandestine operation measures to the Supreme Court does not have to satisfy the element of grounds for suspicion (Croatian: *osnove sumnje*). Still, only the name of the clandestine operation measure, name of the person who will be observed, explanation of the reasons for conducting that measure and the term or duration of measure and it is issued from the Supreme Court judge and not the investigative judge of County Court.¹² In that sense it can also briefly be mentioned that the level of "grounds for suspicion" that the person has committed criminal offence is a legal standard for the application of the special evidentiary measures in the criminal procedure and it has to precede the special evidentiary measures, concretely refer to the committed criminal offence (no speculations). Furthermore, the legal standard points that the specific criminal offence is committed¹³ and those indicate that there could be a significant distinction between special evidentiary measures and clandestine operation measures which are conducted by the intelligence agencies.

IMINT means an intelligence discipline which is related to the collection, analysis and interpretation of pictorial records. FININT means an intelligence discipline which collects and analyzes financial data, respectively by tracking financial activities and the cash flow. GEOINT means an intelligence discipline of collection and analysis of the marks of the geographically defined space (e.g. records of military movement, buildings and satellite images), see more in: Malnar, *op.cit.* note 4, p. 153-174.

¹² Article 36 and 38 of the SIS Act. According to article 332 (1) of the CPA the special evidentiary measures can be pointed only to persons for whom there are grounds for suspicion that they have committed specific criminal offence from the list of article 334. of the CPA, along with other conditions stipulated in the CPA.

¹³ See more in: Burić, Z. et al, *Upotrebljivost rezultata masovnog nadzora komunikacija kao dokaza u hrvatskom kaznenom postupku – slučaj SKY ECC*, Hrvatski ljetopis za kaznene znanosti i praksu, Vol. 30., No.2., 2023., p. 261-262.

Aside above-mentioned clandestine operation measures, intelligence agencies can get in touch with criminal offences and possible evidence during for example oversight of open sources, through informants, recorded conversations with citizens¹⁴ or even during execution of security vetting. Security vetting is a part of preventive work of intelligence agencies which is necessary in order for individual to access classified information or to be appointed to specific public duties.¹⁵ Security vetting is done in accordance with special regulations.¹⁶ If we look at the content of the questionnaire¹⁷ of the security vetting, it is clear that intelligence agencies in that procedure gather wide range of data, for example data on assets, health data, data on prior convictions, previous contacts with criminal offenders, foreign intelligence agencies, telecommunication data etc. It is evident that those data can indicate to possible criminal offence and at least be a basis for conducting the police investigation.¹⁸

Criminal offences relevant to the intelligence agencies are primarily those that satisfy two requirements. Objective element is that the criminal offences pose the threat to the national security while the subjective element is that the perpetrators are directed against the interests of a national security. Those criminal offences are characterized with the high level of organisation, covert action, duration of activities so the optimal way of combat with that crime is with the help of intelligence agencies, which are specialized in the long-term collection of

¹⁴ According to article 27 (2) of the SIS Act, intelligence agencies are authorized to conduct conversations with citizens in the official areas of intelligence agencies. Conversations are technically recorded and the minutes (document) is held while citizens confirm with their signature that the conversation was voluntary, truth and complete.

¹⁵ Croatian Security and Intelligence Agency (hereinafter: SOA) has conducted 6626 security vetting procedures in 2022 (last public report). See: Security and Intelligence Agency, *Annual Report for 2022*, available online via URL: <https://www.soa.hr/files/file/Public-Report-2022-en.pdf> (retrieved on 16th of February 2025).

¹⁶ Security Vetting Act, Official Gazette, No. 85/2008, 86/2012; Data Secrecy Act, Official Gazette, No. 79/2007, 86/2012; Regulation on the content, appearance, filling in and handling of the Security Vetting Questionnaire, Official Gazette, No. 114/2008.

¹⁷ Questionnaire is available online via URL: https://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/2016/I_Degree_Security_Vetting_Questionnaire.pdf (retrieved on 23th February 2025).

¹⁸ Cf. Arslan, who explained that within the system of Turkish Criminal Procedure, it is quite common to utilize intelligence (and data that have similar attributes) in following 5 purposes: a) Utilization of Intelligence before the Perpetration of the Crime (During Pre-Crime Investigation / During Preliminary Inquiries), b) Utilization of Intelligence after the Perpetration of the Crime, for the Purpose of Initiating the Investigation (Suspicion of an Overt Act), c) Utilizing Intelligence for the Purpose of Taking Cautionary Measures, after the Perpetration of the Crime, d) Utilization of Intelligence for the Initiation of Prosecution and e) Utilization of Intelligence for the Sentencing. Arslan, C., *Intelligence in Criminal Procedure Law*, 2013/ 2 Ankara Bar Review, p. 54-56.

data/information, clandestine operation measures and high level of organisation.¹⁹ From the above mentioned it is evident that examples of those criminal offences are mainly from the Chapters IX, XXIV, XXXII and XXX of the Criminal Code.²⁰

2.2. Different sorts of information gathered by intelligence agencies as possible evidence in criminal procedure

Now that we explained some basics of connection between intelligence agencies and law enforcement bodies it can further be elaborated that intelligence agencies can gather different sorts of evidence such as documents, technical recordings, items and personal evidence.²¹

Documents²² can be collected during for example reception of various documents from public bodies and legal persons and can be also made by intelligence agencies for example in the form of minutes from conversation with citizens or when informing beneficiaries in the form of reports.²³

Furthermore, technical recordings²⁴ can be collected during for example clandestine operation measures of oversight and technical recording of closed areas/interior, clandestine oversight and observation with audio recording in open areas/public spaces. It is more than obvious that intelligence can be collected in this sense in textbook case of recorded criminal offence of drug trafficking or even taking bribe or buying a weapon. Intelligence services can also collect information from clandestine operations of clandestine oversight of the content of communication (*e.g.*, SMS, WhatsApp messages, phone calls etc.).

Items can be collected during for example clandestine repurchase of documents and items such as forged documents. At the same time, personal evidence can be

¹⁹ Badžim, J., *op.cit.*, note 5., p. 234-273.

²⁰ Criminal Code, Official Gazette, No. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022, 114/2023, 36/2024 (hereinafter: Criminal Code). For example: Treason, Giving/receiving bribes in business dealings, Recruitment of mercenaries, Terrorism, Financing of Terrorism, Criminal Enterprise etc.

²¹ Badžim J., *op.cit.* note 5, p. 326.

²² Documents represent any record which contains a set of linguistic signs with a specific meaning content that serves to establish facts in criminal proceedings, Krapac, D., *op. cit.*, note 4, p. 508.

²³ See provisions of articles 25, 27 and 55 of the SIS Act

²⁴ Technical recordings can be photos, recordings, audio and television photo records, Krapac, D., *op.cit.*, note 4, p. 515.

broad from information from citizens, intelligence agents or even informants.²⁵ All of them can be possible witnesses in the later stage of criminal proceedings.

3. LEGAL OBSTACLES AND CREDIBILITY ISSUES TO USING INTELLIGENCE DATA IN CRIMINAL PROCEEDINGS

Intelligence data have numerous credibility issues regarding its possible use in criminal proceedings. One of the main general challenges and obstacles is that intelligence data is collected for the purpose of protection of national security which generally results in the confidentiality of such data. Collected intelligence data is the ownership of intelligence agencies so they can classify that data with one of the four levels of classification (top secret, secret, confidential and restricted). Right of access to documents (top secret, secret, confidential) can be realized only if that is necessary for the execution of public tasks and with the security clearance²⁶, while the access to restricted documents can be accessed if that is necessary for the execution of public tasks and with the security informing.²⁷ In the criminal procedure there is a possibility that the court or the state attorney request the intelligence agency to declassify intelligence data but the intelligence agencies as data owners of data reach a decision will the data be declassified or not and intelligence agencies have to ask an opinion on the declassification from The Office of the National Security Council.²⁸ In that sense it can also be mentioned that aside documents, for example personal evidence (testimony of intelligence agents) is an obstacle in criminal proceedings since intelligence agents are obliged to keep as a secret all data which they have found out during clandestine operation measures so they are relatively incapable for witnessing as long as they are obliged to keep a secret (they can be relieved that obligation from the intelligence agency) and to protect public interest which is stronger than the interest of criminal procedure.²⁹ Secrecy is mandatory since intelligence agencies cannot afford to reveal information what do they know and how they acquired information to the for example terrorists (as possible

²⁵ According to article 29. of the SIS Act intelligence agencies are authorized to collect data from informants/secret associates.

²⁶ See provisions of articles 2, 4 and 18 of the Data Secrecy Act.

²⁷ See Article 4 (2) of the Regulation on information security measures, Official Gazette No. 46/2008.

²⁸ See Article 264 of the CPA and Article 16 of the Data Secrecy Act.

²⁹ See Article 284 of the CPA; Krapac, *op. cit.*, note 4, p. 488.

defendants) because they would change their behaviour and possibly endanger national security and perform terrorist attack.³⁰

Furthermore, intelligence agencies have the main mandate to inform its end users of possible threats to the national security so the end users (for example, State president, prime minister, ministers, public officials³¹) can develop and reach decisions for the protection of national security.³² So, they are not assigned with the task of criminal prosecution but informing end users through the various reports as the final product of the intelligence cycle.³³ Those reports can be in written or oral form and they contain accurate intelligence data about possible threats to national security to end users and they represent the final stage of intelligence cycle which must be made in the manner so the end users can make political decisions based on information which are processed with the help of intelligence analysts.³⁴ From the above mentioned it can be concluded that such reports do not contain information which is relevant for criminal proceedings namely because they are not intended for that purpose. Another obstacle in that sense which can compromise credibility of such evidence is that original or raw documents, items, records *etc* can be processed in different ways so they no longer present original data³⁵ and their originality as well as accuracy and integrity may be put in question. Furthermore, intelligence agencies have a duty to protect its sources and methods of work. That could be another problem in the sense of credibility of intelligence reports as possible evidence in criminal proceedings so even the reports cover all data which are not necessary to the needs of end users.³⁶ In that sense it can also be written that those reports mostly rely on statements of the individuals who are not being questioned by the court or the accused, so those reports constitute hearsay evidence and rely on anonymous/protected sources so their reliability is questionable.³⁷

Besides final reports, there are also authentic intelligence data which is made at the first stage of intelligence cycle or during the collection of data³⁸. Those data

³⁰ Waxman, C. M.; Barak Erez, D., *Secret Evidence and the Due Process of Terrorist Detentions*, Columbia Journal of Transnational Law 3, 2009, p. 5.

³¹ Malnar, *op.cit.*, note 4, p. 196-198.

³² Hasanovic, A. *et al*, *Nacionalna sigurnost Republike Hrvatske u 21. stoljeću – knjiga 2*, Jesenski i Turk, Zagreb, 2023, p. 86-88.

³³ Intelligence cycle represents the process of planning, collecting, analysing and distribution of intelligence data to end users. Tudman, M.; Akrap, G.; Matošić, V., *Leksikon izvještajnog nazivlja*, National Security and the Future, 1-2 (22), 2021., p. 145.

³⁴ See more in: Malnar, *op. cit.*, note 4., p. 193-210.

³⁵ See more in: Badžim, *op. cit.*, note 5, p. 418-419.

³⁶ *Ibid*, p. 405.

³⁷ See more in: Vogel, B., *Secret Evidence in Criminal Proceedings*, Max Planck Institut für ausländisches und internationales Strafrecht, Duncker & Humblot, Berlin, 2021, p. 19.

³⁸ They are not yet processed by analysts and put in form of final report to end users

are "raw" and can contain data which are of interest for the public prosecutor since they can better express details which are of interest to the proving of criminal offence and the perpetrator (for example video records of committed criminal offence). But those data are mainly intended to the internal reporting of intelligence agencies. Those reports still have a problem with secrecy of the intelligence sources so the problem of credibility still exists.³⁹ Another obstacle to the possible use of such data as evidence in criminal proceedings can be encryption of the data since criminals usually use encryption methods during communication which is intercepted. Therefore, in the criminal proceeding there can be a necessity to conduct the expertise in order to adequately understand the content of communication.⁴⁰

Intelligence agencies informants can have some valuable information and their testimony as witnesses in court could also be possible evidence in criminal procedure but there is always a problem of credibility since the informants usually come from criminal circles.⁴¹ For the assessment of the credibility of that evidence it can be mentioned that for example police have four levels of credibility of informants; reliable source, mostly reliable source, mostly unreliable source, indeterminate source (depends mostly on the accuracy of the former information given to law enforcement bodies).⁴²

4. ANALYSIS OF THE LEGAL GROUNDS FOR THE POSSIBLE USE OF INTELLIGENCE INFORMATION AS EVIDENCE IN CRIMINAL PROCEEDINGS IN THE REPUBLIC OF CROATIA

The legal framework in the Republic of Croatia does not provide a clear answer as to which results of the work of security and intelligence services could be used as evidence in criminal proceedings. Moreover, the above-mentioned issue is not mentioned at all in the main acts that are supposed to resolve these issues, with the exception of Art. 187 (5) of the CPA. Apart from the above provision, the CPA only mentions security services in relation to legal aid in Art. 191, which has no

³⁹ Badžim, *op.cit.*, note 5, p. 327.

⁴⁰ See more about encryption methods in: Čukljaš, Đ., *Tajno komuniciranje špijuna*, Ministarstvo unutarnjih poslova, Zagreb, 1994.

⁴¹ According to some sources, one third of criminal offences cannot be solved without the help of informants, , at least in the first stages of criminal investigation which is usually conducted by the police. See more in: Karas, Ž., *Uvod u kriminalistiku*, Ministarstvo unutarnjih poslova, Zagreb, 2012, p. 162., See more about credibility of witnesses in general in: Krapac, *op.cit.*, note 4, p. 500.

⁴² See article 54 of the Police Rulebook.

connection with the problem under consideration. The Act on the State Attorney's Office and the Act on the Office for the Suppression of Corruption and Organized Crime mention security services exclusively in the context of security checks during employment, while the Rules of Procedure of the State Attorney's Office, apart from the above, only in the context of secrecy or classification of data (Art. 79). The same is true in the Act on Courts, the Act on Police Affairs and Powers, and the Act on the Police.

On the other hand, the Act on the Security Intelligence System of the Republic of Croatia (SIS Act) does not mention the word "evidence" anywhere, nor the term "criminal proceedings" in the context that could be expected for a body that could often have valuable information about perpetrators of certain criminal offences. Only in Articles 18 and 20 of SIS Act is the CPA mentioned, but in the sense of establishing the OTC⁴³ and other technical issues. The main point of contact between SIS Act and criminal proceedings is Article 56 of SIS Act, which establishes the duty of security intelligence agencies to notify the State Attorney's Office if the information collected indicates the preparation or commission of a criminal offence that is prosecuted ex officio. Paragraph 2 of that article stipulates the exceptional possibility that the aforementioned notification may also contain information on the method of data collection.

This state of the laws leaves us very little room for reaching a conclusion about the usability of the results of the work of the security intelligence services as evidence in criminal proceedings, but it offers us at least some starting point. Even in the scientific literature, the situation is not much better. Very little has been written about the mentioned problem, mostly without offering specific answers. The most important statement of domestic authors on this issue can be found in the textbook of criminal procedural law, which has not been changed for the last twenty years. Thus, Krapac states that the technical recordings obtained by measures of secret data collection for the purposes of national security, which are obtained by officers of the security-intelligence agency based on a written reasoned order of the judge of the Supreme Court of the Republic of Croatia, cannot be used as evidence in criminal proceedings without further ado, because

⁴³ Operational and Technical Center for Telecommunications Supervision (Croatian: Operativno-tehnički centar za nadzor telekomunikacija), an operational-technical body that, in the performance of tasks from its scope of work prescribed by the Act on the Security and Intelligence System of the Republic of Croatia, communicates with bodies authorized to apply measures of secret telecommunications surveillance and telecommunications operators. <https://www.otc.hr/>.

the state attorney is only exceptionally informed about the method of data collection and the results of such measures.⁴⁴

Krapac warns that those recordings are kept as the strictest secret. However, the court could use such secret technical recordings of security and intelligence agencies in criminal proceedings only after the approval of the competent authority in accordance with the provisions of the current law regulating the issue of data confidentiality.⁴⁵ The above understanding is interesting for analysis in many ways. Namely, Krapac nowhere mentions restrictions on the criminal offenses for which such evidence could be used. Since the SIS Act has not been amended since 2006, based on the provisions of its Art. 56, it should be taken to mean all criminal offenses for which prosecution is carried out *ex officio*. Furthermore, the author speaks of technical recordings that were created on the basis of a written and reasoned order of a Supreme Court judge. Unfortunately, he does not state anything about technical recordings that would be created by secret measures determined by the director of the Intelligence Agency, and without a court order under Art. 38 of the SIS Act. The above issue can potentially be of great importance if the existence of an order from the judicial authority is taken as a criterion for the legality or usability of the results of the actions of security and intelligence services.

Among other authors, Badžim should be highlighted, who has dealt with this issue in more detail. He examines in detail all the actions and measures of the security and intelligence services and their evidentiary potential, and in principle he is in favour of the legality or illegality of certain evidence that is the result of the work of the security and intelligence bodies, but without establishing any clear criteria, he advocates leaving specific cases to judicial practice and free assessment of evidence. It is not possible to enter into a detailed polemic about everything presented here, but for the purposes of this paper it is sufficient to state that Badžim unequivocally declares himself in favour of the possible use of the results of the work of the security and intelligence services as evidence in criminal proceedings, whereby the courts will have to address the issues of fairness of the procedure, the legality of such evidence and its credibility in each specific case.⁴⁶

⁴⁴ Krapac, D. et al., *Kazneno procesno pravo*, Prva knjiga, institucije VIII. amended and supplemented edition, Narodne novine, Zagreb, 2020, p. 510, footnote 210.

⁴⁵ Ibidem. The same position is found in earlier editions of the book, including the 2007 edition. The author states that approval from the competent authority is required in accordance with the provisions of the Protection of Data Secrecy Act. The aforementioned Act was passed in 1996, and was replaced in 2007 by the Data Secrecy Act, which is currently in force and amended in 2012. Since there have been many changes in relation to the observed issues during that period, the aforementioned understanding should be taken with caution.

⁴⁶ Badžim, J., *op. cit.*, note 5.

Case law is very scarce. We will mention two court decisions.⁴⁷ In 2007, the first-instance court presented at the hearing, for the criminal offense of drug abuse – from Art. 173 (2) of the Criminal Code, evidence obtained by reading the printouts of mobile phone and telephone numbers from the SOA,⁴⁸ while in 2012, the Supreme Court of Croatia concluded that the evidentiary proposal to obtain from the SOA and the Ministry of Internal Affairs data on the criminal processing of A. M. in connection with the murder of I. H. was correctly rejected because this data cannot be used as evidence in these proceedings.⁴⁹ In any case, a broader analysis of case law on this issue would be desirable in some future research.

Since only Art. 187 (5) of the CPA offers some answers, it is necessary to analyze the text of the legal provision. It should be emphasized right away that the aforementioned provision refers only to criminal offenses from the catalogue that is an integral part of the provision. This section does not address the content of the catalogue, which refers to the narrowest area of interest of security and intelligence services, and has been somewhat changed since 2008. to the present day through amendments to the CPA. It is sufficient to state that this provision does not apply to the vast majority of criminal offenses at all. Therefore, personal data used to determine the identity of the defendant, collected by security and intelligence services, can exceptionally be used as evidence in cases for criminal offenses from the catalogue. At first glance, the observed provision is not so simple for drawing conclusions, and it is necessary to analyze it logically. Given everything previously stated in our literature, the assumption is that this provision represents only a fragment in the broader picture of the use of the results of the work of security and intelligence services as evidence in criminal proceedings.

The first conclusion that arises from the analysis of the observed provision is that personal data used to establish the identity of the defendant, collected by intelligence services, cannot be used as evidence for acts not listed in the catalogue, and for acts from the catalogue only exceptionally.⁵⁰ If we relate the

⁴⁷ The authors tried to find the relevant judgment by searching available sources of court decisions on search engines available on the websites <https://odluke.sudovi.hr/>, the Constitutional Court website, and the case law search engine on the IusInfo portal. The keywords and parts of the words "SOA" "obavještajn.." "sigurnosn.." were used as search criteria, and only these two decisions were found.

⁴⁸ VSRH I Kž 705/2008-5 of 3. March 2010.

⁴⁹ I Kž-Us 22/11-11 of 8. February 2012.

⁵⁰ The meaning of the expression "exceptionally" could be interpreted differently. It is possible that the aforementioned exceptionality is exhausted in the fact that for other criminal acts the observed data cannot be used, but can be used for criminal acts from the catalogue. If we consider that for crimes not in the catalogue, this data cannot be used as evidence, and for crimes in the catalogue, it can only be used exceptionally, it is still not entirely clear what this exceptionality means. Does it refer to the fact that the identity cannot

aforementioned conclusion to the provision of Art. 56 of the ZSOS, it follows that intelligence services must report to the state attorney on the collected data related to all criminal acts prosecuted *ex officio*, but if this data relates to personal data on the identity of the defendant, then it cannot be used as evidence in criminal proceedings, except for catalogue criminal acts for which this can only be done exceptionally.

However, everything stated in Art. 187 (5) of the CPA tells us nothing about other data collected by security and intelligence services in their work, which do not fall into the category of personal data. If personal data can only be used exceptionally, does this mean that other data can be used for evidentiary purposes without exception? Or, conversely, does it mean that other data cannot be used exceptionally? We also do not know whether the catalogue of criminal offences from Art. 187 (5) of the CPA also refers to other data on criminal offences or only to the aforementioned personal data. After all, how can we make a clear distinction between the data obtained in terms of whether they contain personal data on the identity of the defendant or "only" some other data?

If we start from the previously mentioned concept according to which the results of the work of security and intelligence services could be used as evidence if the authorized body removes the classification mark from the obtained data, then we could say that the "exception" from the provision of Art. 187 (5) of the CPA refers to declassification. However, this again does not give us an answer as to what happens with other data that does not relate to identity. Logically speaking, a closer solution would be that other data could be used as evidence if the authorized body removes the classification mark, because strictly personal data is "more protected" than ordinary data. Such an interpretation pushes us further into deeper problems. Namely, does the catalogue from Art. 187 (5) of the CPA also apply to other data? The impression is that there is such an expectation, but this simply does not follow from the aforementioned article of the CPA. The logical and consistent regulation according to which the security and intelligence services of the state attorney must report on collected data related to all criminal offenses prosecuted *ex officio* does not work, and this data can only be used as evidence if the classification is removed from it, whereby the catalogue of criminal offenses applies to personal data, and this catalogue does not apply to other data.

The concept of the broad possibility of applying the results of the work of security and intelligence services as evidence in criminal proceedings, whereby the courts

be established in any other way, or does it depend on whether the data will be declassified, which will only happen exceptionally.

will in each specific case have to deal with issues of the fairness of the proceedings as a whole, and judge and weigh the issue of the legality of the evidence obtained and its credibility, is also not easy to reconcile with the provision of Art. 187 (5) of the CPA. Namely, it is unclear whether such a concept should be applied only to criminal offences from the catalogue or even more broadly. The impression is that there is again an expectation that the concept should be applied only to criminal offences from the catalogue, since the aforementioned criminal offences fall within the focus of the work of security and intelligence services, and that expanding its application for evidentiary purposes to criminal offences that are not in the catalogue would be unacceptable from the point of view of the principle of fairness, i.e. it would represent an overly broad intrusion into the privacy of the defendant.

If we look at the problem in terms of content and applying only legal logic, the provision of Art. 187 (5) of the Criminal Procedure Code refers only to establishing the identity of the defendant, and not generally to the commission of a criminal offense, which is a broader concept. Therefore, the catalogue of criminal offenses from the aforementioned article refers only to the issue of establishing the identity of the defendant. Security and intelligence services gain knowledge about all criminal offenses through their work, and the issue of applying the results of such knowledge as evidence in criminal proceedings should be resolved outside the provisions of Art. 187 (5) of the Criminal Procedure Code. Such a broad scope, outside the "catalogue", is very controversial. Namely, if we look only at the application of measures for secret data collection from Art. 33 of the SIS Act, we indirectly open up the possibility of applying such data as evidence even more widely than the application of the results of special evidentiary actions carried out in accordance with the provisions of the CPA, for which there is a clear catalogue in Art. 334 of the Criminal Procedure Act. It is quite clear that such a thing is unacceptable.

The solution could be sought within the framework of "weighing" or the application of Art. 10 (3) of the CPA, whereby the application of evidence originating from security and intelligence sources would not be possible for criminal offences under the jurisdiction of the municipal court, or would possibly only be possible for serious forms of criminal offences under the jurisdiction of the county court, where the interest of criminal prosecution and punishment outweighs the violation of rights. It is unlikely that the legislator opted for a solution that relies in advance on the application of evidence obtained by violating the rights and freedoms under Art. 10 (2) of the CPA, but will still be declared

lawful due to "weighing".⁵¹ On the one hand, such an approach is frivolous from the aspect of the efficiency of criminal prosecution, and on the other hand, it would simply have to be contrary to the Constitution of the Republic of Croatia, if we look at the whole matter from the aspect of fairness.⁵²

If the legislator intended to broadly allow the use of the results of the work of security services as evidence in criminal proceedings, the concept of only fragmentary disclosure of personal data relating to the identity of the defendant is completely unclear. Regardless of whether the emphasis is on the issue of declassification or leaving it to the court to judge and decide in each specific case on the issue of the legality of the evidence obtained or the fairness of the treatment of the defendant as a whole, the current legal framework is not good.

Finally, it is necessary to consider whether the earlier assumption that the provision of Art. 187 (5) of the CPA is only a fragment in the broader picture of the use of the results of the work of security and intelligence services as evidence in Croatian criminal proceedings is actually completely wrong. It is necessary to consider the understanding according to which the aforementioned provision provides us with a complete legal framework. Namely, a restrictive interpretation of the completely exceptional application of the results of the work of security and intelligence services as evidence in criminal proceedings does not lead us to the problems presented earlier. The aforementioned interpretation would be reduced to the fact that the results of the work of security and intelligence services cannot be used as evidence in criminal proceedings, except exceptionally. The aforementioned exception is prescribed precisely by the provision of Art. 187 (5) of the CPA. Therefore, only if the identity of the defendant cannot be established in any other way, and it concerns a criminal offense from the catalogue, it is possible to establish the identity of the defendant on the basis of personal data obtained through the work of intelligence services.⁵³ It is reasonable to assume that in the above case, too, the issue of data confidentiality must be taken into account.

⁵¹ It is difficult to imagine what problems the court may encounter if we take into account issues related to, for example, incidental findings modelled on special evidentiary actions or the doctrine of the fruits of the poisonous tree.

⁵² It is interesting in this sense the understanding of Grubač, who, commenting on a factually identical problem in Serbia, considers any use, including legal regulation of the use of evidence obtained by secret services, to be illegal and ultimately contrary to the Constitution, in violation of the current law on criminal procedure. Cf. Grubač, M., *Krivično procesno pravo*, Law Faculty of Union University in Belgrade, Belgrade 2008, p. 248.

⁵³ Garačić and Novosel state that the provision of Art. 187 (5) of the CPA generally refers to cases of arrest of persons for whom there is reasonable suspicion that they have committed one of the offences from the catalogue, and whose identity cannot be established on the basis of existing records kept in the Republic of Croatia or in another country. Garačić, A.; Novosel, D., *The Law on Criminal Procedure in Judicial Practice - Book One*, Libertin Publishing House, Rijeka 2018, p. 467.

The provision of Article 56 (1) and (2) of the SIS Act could be interpreted in the same sense. Namely, if the collected data indicate the preparation or commission of a criminal offense that is prosecuted *ex officio*, security intelligence agencies report to the state attorney's office. This notification may exceptionally contain information on the method of data collection. Therefore, there is a duty to report to the state attorney about all criminal offenses, but security intelligence services only provide complete information that could be used as evidence in exceptional cases. It is precisely in Article 187 (5) of the CPA that the exception is made, namely data on the identity of the defendant in the case of criminal offenses from the catalogue. For other criminal offenses, evidence of identity may not be officially provided, but only "bare" information about the criminal offense, and the state attorney must proceed further and prove it, if possible, according to the rules of the CPA.⁵⁴

Such a restrictive interpretation is justified by the very purpose of the activities of security and intelligence services. Their work is not aimed at proving or obtaining evidence, but at pure knowledge without formal traces. They oppose crime by (secret) knowledge, not by proving it. Security and intelligence services collect data, establish and maintain collections and registers of personal data and other records, in accordance with Article 39 of the SIS Act, and this data constitutes a strictly guarded secret. The provision of Article 187 (5) of the CPA, as well as the provision of Article 39 of the SIS Act, speak predominantly about personal data. Furthermore, it has already been pointed out that the SIS Act does not mention the term evidence at all, but speaks exclusively about data. For example, Article 33 of the SIS Act speaks about measures for the secret collection of data if the data cannot be collected in any other way or their collection is associated with disproportionate difficulties. The justification for such an interpretation can be seen in the example.

To put it simply, the provision of Art. 18. of SIS Act established the Operational and Technical Centre for Telecommunications Surveillance (hereinafter: OTC), in order to perform tasks related to secret surveillance measures over telecommunications for the purposes of applying special evidentiary actions according to the CPA and secret surveillance measures according to Art. 33. of SIS Act. For example, a secret recording of the content of a telephone conversation can be viewed, from which it appears that the subject being monitored has committed a criminal offense. If the mentioned recording was created as a result

⁵⁴ In certain complex cases, the directors of security and intelligence agencies may propose to the Attorney General to postpone further action within his jurisdiction if this would jeopardize the further execution of tasks within the scope of the security and intelligence agencies or the safety of employees and sources of security and intelligence agencies (Art. 56 (3) of the SIS Act).

of a special evidentiary action from Art. 332. (1) (1). CPA, approved by the investigation judge at the request of the state attorney, in terms of criminal procedural law, it is a technical recording as evidence on which a conviction can be based. However, if the exact same recording was created as a result of the secret data collection measure from Art. 33 (3) (1) a of SIS Act, approved by a judge of the Supreme Court of the Republic of Croatia at the request of the director of the security and intelligence agency, then in terms of criminal procedural law it is not a technical recording as evidence. It can be said that the said recording does not actually exist for the criminal proceedings body. It is the subject of processing and analysis by the security and intelligence agency, and the result of that analysis is data that is entered into collections and registers of personal data and other records, in accordance with Art. 39 of SIS Act, and this data constitutes a strictly guarded secret. The state attorney or the criminal proceedings body may only receive such "bare" data, and only exceptionally may the report contain data on the method of data collection, if it is a case from Art. 187 (5) of the CPA.

5. A BRIEF COMPARATIVE LAW ANALYSIS OF SOME REPRESENTATIVE EUROPEAN COUNTRIES

Although comparative law analysis will be the subject of a separate article, here we will give a brief overview of some comparative law solutions in the Netherlands and the United Kingdom that allow the use of intelligence agency information in criminal proceedings.

These two countries were chosen because, unlike most other European countries, they have introduced provisions in their criminal legislation that enable the use of intelligence services as evidence in criminal proceedings. Another reason is that they do it in different ways, thus representing two different models; The Netherlands through special examining magistrates and the United Kingdom by appointing special advocates.

5.1. Netherlands

In the Netherlands (as in the vast majority of European countries) there is a strict separation between the intelligence agencies and the public prosecutor's office. These organizations work under their own legal regime, have different tasks, powers and responsibilities. Yet, legal provisions provide possibility of "intensive

information flow between them".⁵⁵ In case of terrorist crimes, intelligence information that could be useful for the investigation and prosecution can at the discretion of the Dutch General Intelligence and Security Service (AIVD) be provided to the Netherlands Public Prosecutor Service in the form of official written report (Dutch: *Ambtsbericht*) that contains testimonies by officials and informants.⁵⁶

But now the question arises of the possibility of using such information as evidence in criminal proceedings. In order to create the possibility of using such information as evidence, in September 2006 the Dutch legislator passed the "Act on Shielded Witnesses" (Dutch: *Wet Afgeschermde Getuigen*). This Act opens the possibility of questioning a protected witness, an employee of the intelligence service, in a special procedure in the pre-trial phase, *ex parte* and *in camera*, in case disclosure of the identity of the witness could endanger the witness or national security.⁵⁷ These witnesses are examined by a 'special' examining magistrate (Dutch: *Rechter-Commissaris*). It is his duty to decide whether, in the interest of national security, particular information must remain secret and whether the identity of witness should be kept secret. A special section of the Rotterdam District Court is in charge for this procedure in pre-trial phase. As a rule, the trial participants are not present during shielded witness hearing, but they can give a list of questions for the witness to the special examining magistrate.⁵⁸

Since the European Court of Human Rights has warned in several of its decisions that a conviction cannot be based exclusively or predominantly on the testimony of a witness whom the defense has not had the opportunity to examine, Article 344a of the Dutch Code of Criminal Procedure also stipulates that "the court may not find that there is evidence the defendant committed the offence as charged in the indictment exclusively or to a decisive extent on the basis of written materials containing statements of persons whose identity is concealed". Therefore, Eijkman and van Ginkel, warn that "this is a crucial concern in relation to the Act" because the officers of Dutch General Intelligence and Security Service (AIVD) "will hardly ever be able to produce any extra information that supports the official written report that is submitted as evidence".

Described provisions could be described as an attempt to reconcile the need to use extremely valuable intelligence information as evidence in criminal proceedings with the requirements of the principle of fair procedure. Yet, number of human

⁵⁵ Eijkman, Q.; Van Ginkel, B., *Compatible or incompatible intelligence and human rights in terrorist trials*, Amsterdam Law Forum, 3(4), 2011, p. 8.

⁵⁶ *Ibid.*

⁵⁷ *Ibid.*

⁵⁸ *Ibid.*, p. 9.

rights concerns remain, one of the most important being the fact that in testing reliability and lawfulness, the trial judge has to rely completely on the marginal assessment of the examining magistrate.⁵⁹ Not only trial judge, but also the defence counsel need to rely completely on the work of special examining magistrate.⁶⁰

5.2. United Kingdom

As another example of a comparative legal system that has adopted legislative changes to enable the use of intelligence information in criminal proceedings, we have chosen United Kingdom. The reason for this is that the British legislator has chosen a somewhat different model of reviewing this information before it is included in the evidence. While the Netherlands has entrusted this task to examining magistrates, in United Kingdom the so-called special advocates play a significant role in the process of evaluating intelligence in criminal trials.⁶¹

In UK, this institute has its roots in immigration law and introducing the appointment of a special advocate in deportation proceedings on national security grounds. After the European Court of Human Rights ruling in the case of *Chahal v. UK*,⁶² the legislator introduced Special Immigration Appeals Commission Act

⁵⁹ Vervaele, J. A. E., *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?*, International Review of Penal Law (Vol. 76), p. 441.

⁶⁰ Eijkman, Q.; Van Ginkel, B., *op. cit.*, note 55., p. 9-10. Eijkman and van Ginkel also rightly emphasize the problematic situation where the intelligence data had been collected not by Dutch AIVD, but by foreign intelligence agency and then just given to AIVD.

⁶¹ Some authors state that the United Kingdom (UK) is a pioneer with regard to counter-terrorism legislation because of its history and that its legislative response had been initiated because of the terrorist crimes of the Irish Republican Army, Sinn Féin and the Ulster Freedom Fighters. Bennet, G., *'Legislative Responses to Terrorism: A View from Britain'*, The Penn State Law Review 2005-109, No. 4, pp. 947-966., as cited in: Eijkman, Q.; Van Ginkel, B., *op. cit.*, note 55., p. 14.

⁶² *Chahal v. United Kingdom*, App. No. 22414/93. In this very significant case, ECtHR prohibited member states of the Convention from deporting people to other countries if they would be exposed to the risk of being tortured there. On importance of this case on the development of the British special advocate system, see: Jenkins, D., *There and Back Again: The Strange Journey of Special Advocates and Comparative Law Methodology*, Columbia Human Rights Law Review 42, 2011, pp. 282-288. In its decision, the ECtHR was guided by the example of Canada, which was the first to start with the model of using special advocates. However, Jenkins, analyzing in detail that ECtHR decision and the law and practice of Canada, warns that the stated analysis of special advocate system was inaccurate in three important respects. He states that "the ECHR therefore not only overlooked three important limitations built into the Canadian special advocate system itself, but failed to make any macro-comparison whatsoever between the two national legal systems". *Ibid.*, p. 300-301.

of 1997. (SIAC Act) which authorises such appointments. Special advocates are lawyers, appointed to represent the interests of defendants in circumstances where sensitive information may need to be withheld from them in the name of national security. This mechanism has primarily been implemented in the realm of terrorism-related cases, where trials often contain classified evidence that the accused cannot access.⁶³

Justice and Security Act of 2013 has defined the authority and procedures for appointing these advocates while balancing national security interests with the rights of defendants under common law and human rights legislation.⁶⁴

It must be emphasized that the special advocate may not communicate with the appellant once he or she has received the secret information. That is one of the biggest concerns regarding the respect of fair trial principle. Although opinions differ on this, the authors believe that it is difficult to say that it is a matter of full compliance with Art. 6 of the European Convention on Human Rights in that case.⁶⁵

6. SOME PROPOSALS REGARDING POSSIBLE LEGISLATIVE CHANGES IN ORDER TO INCREASE THE POSSIBILITY OF USING INTELLIGENCE DATA IN CRIMINAL PROCEEDINGS WITHOUT HARMING FAIR TRIAL PRINCIPLE

After the above analysis, it can be concluded that there are certainly certain difficulties in using intelligence data in criminal proceedings that pose barriers to the use of such data as evidence in criminal proceedings. Intelligence data is a valuable source of knowledge that is useful in directing criminal investigations, i.e. in the initial stages of criminal investigations when criminal proceedings have not yet been formally initiated, since intelligence agencies have, by narrative, significantly broader capacities than criminal prosecution bodies in terms of a multidisciplinary approach to resolving issues within their jurisdiction, i.e. the

⁶³ When information is withheld from the appellant on national security grounds, the special advocate is appointed by the UK Attorney General.

⁶⁴ Section 9 of Justice and Security Act of 2013, available at: <https://www.legislation.gov.uk/ukpga/2013/18/section/9>

⁶⁵ The Joint Committee on Human Rights issued their report on Counter-Terrorism Policy and Human Rights in 2011 and warned that the use of secret evidence and special advocates in United Kingdom needs an "urgent and comprehensive review in all contexts in which they are used". As cited in: Eijkman, Q.; Van Ginkel, B., *op. cit.*, note 55. p. 14.

ability to perceive security threats, which can at the very least direct criminal prosecution bodies and thus significantly assist them in collecting evidence for the purposes of criminal proceedings.

On the other hand, the structure of contemporary crime is such that there are increasingly cases in which it is difficult to prove the commission of certain serious crimes dangerous to the community without using information collected by intelligence services. Therefore, bearing in mind the limited scope of this paper, we will present below some individual proposals that should be considered when making possible amendments to the law if we wish to use intelligence services' information to a greater extent in criminal proceedings. Therefore, the following ideas and proposals, without any pretensions to completeness, are by no means the most important or the only ones, but merely food for thought before a more comprehensive treatment of the aforementioned issue.

6.1. Possible limited changes to the rules on admissibility of evidence in the Criminal Procedure Code

Taking into account that intelligence data is a valuable source of information about perpetrators and criminal acts, namely the above-mentioned serious criminal acts that are characterized by permanence, concealment and organization, it could also be considered to introduce a more precise normative exception into the Criminal Procedure Code and prescribe that in the event that there is no other evidence about the committed criminal act and the perpetrator, evidence collected by intelligence agencies may exceptionally be used in criminal proceedings, which, among other things, indicate sources of information about the committed criminal act and perpetrators, and only in relation to catalogued serious criminal acts based on Article 187 (5) or *de lege ferenda* its proposed regulation with the previously stated expansion of security checks, but on the condition that the content of such evidence and its credibility in terms of confrontation and the right to equality of arms can be appropriately reviewed by the defense, so as not to undermine the fairness of the proceedings as a whole.⁶⁶ The advantage of a special provision in criminal procedural law instead of individual court interpretations based on

⁶⁶ As stated, the practice of the ECHR on the issue of admissibility of data obtained by intelligence services will be analyzed in a future article, but it can already be stated that the Croatian legislator should not be satisfied with only respecting the minimum standards set by the European Court of Human Rights, because, as Đurđević points out, the rules which are set up by the European Court of Human Rights on admissibility of evidence are actually quite low. Đurđević, Z., *Admissibility of evidence, judicial review of the actions of the European public prosecutor's office and the protection of fundamental rights. Protecting fundamental and procedural rights from the investigations of OLAF to the future EPPO* / edited by Valentina Bazzocchi, 2014, p.126.

general rules is also pointed out by Jimeno Bulnes, who states that „an explicit provision in the Criminal Procedure Act would also be desirable... Such specific provision appears more essential when a new form of evidence (even when close to expertise) is appreciated and defended by judicial practice and scholarship, taking into account the fundamental rights that are at stake.”⁶⁷

In conclusion, it can be stated that the subject of interest of intelligence agencies is the supervision of extremely serious forms of illegal actions that threaten national security and that can potentially take deep root in government structures and, in addition to the government, threaten the security of the territory of the Republic of Croatia and its inhabitants as state elements.⁶⁸ Omitting such regulation would make it more difficult to prove criminal acts that are inherent in today's society, especially in the area of organized crime, qualified forms of cybercrime and war crimes in the broader sense of the word, as well as terrorism and criminal acts against state security, the proof of which inevitably requires appropriate engagement of intelligence agencies and proactive action, with mandatory respect for all principles of criminal procedural law, especially the principles of fair trial and, in this regard, equality of arms, confrontation and the right to privacy of the defendant.

It was also stated in the Final Report of the Council of the European Union on Anti-Terrorism from 2004, in which it was essentially emphasized that it is extremely important to ensure the use of intelligence data as evidence in criminal proceedings in terrorist cases by the member states of the European Union, all in order to strengthen the national capabilities to fight terrorism,⁶⁹ and the above certainly applies to other serious criminal offenses that, among other things, threaten national security, especially taking into account that these are criminal offenses which are difficult to prove, and which have incalculable consequences on the fundamental elements of the state. Therefore, one should certainly keep in mind the reflections of the professor Damaška, who emphasized that in situations where the focus of interest is shifted only to ensuring human rights in criminal proceedings, then the proceedings become neurotic. This part will end with a quote from the Damaska: "...a fair procedure would be a procedure that finds an

⁶⁷ Jimeno Bulnes, M., *The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama*, New Journal of European Criminal Law, 8(2), 2017, p.187.

⁶⁸ See more at: Lalović D., *Suverena država – temeljni pravno-politički projekt moderne* (2), Politička misao, Vol. XLII, No.3, 2005, p. 28.

⁶⁹ Council of the European Union - Final report on the Evaluation of National Anti-Terrorist Arrangements, 18th November 2005, available online via URL:

https://www.eumonitor.eu/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vi3aoj3pl4xq/f=blg6836.pdf (accessed 11th March 2025).

*acceptable balance between the need to protect society from crime on the one hand and the need to protect human rights on the other."*⁷⁰

6.2. Security checks for procedural subjects as a prerequisite for participation in the part of the criminal proceedings dealing with evidence collected by intelligence services

A possible solution for evidence dmissibility of inteliigence data could be the expansion of the security check system to judges and prosecutors working on serious criminal offences,⁷¹ which it is advisable to specify in a taxonomic - catalogue manner,⁷² so that they are security checked for processing sensitive data and in this sense, perhaps considering introducing security checks for lawyers who would be on the list of lawyers on duty in proceedings for such serious criminal offences and who would have full rights to challenge and confront such evidence and the right to access the secret case file, which would more easily meet the standards of the principle of fair trial, especially the right to confrontation and to examine prosecution witnesses, in the context of the case law of the European Court of Human Rights. In this regard, one could additionally refer to the already described example of Great Britain.⁷³ Such legislative solution ensures that intelligence agents as witnesses are also cross-examined and that secret information is not revealed to the defendants and their regular lawyers.⁷⁴ The defendant's ability to challenge the testimony of a prosecution witness is the

⁷⁰ Damaska M., *Dokazno pravo u kaznenom postupku: oris novih tendencija*, Pravni fakultet u Zagrebu, 2001, p. 8.

⁷¹ Pursuant to Article 37 (7) of the Courts Act (Official Gazette, No. 28/2013, 33/2015, 82/2015, 82/2016, 67/2018, 126/2019, 130/2020, 21/2022, 60/2022, 16/2023, 155/2023, 36/2024), only judges and civil servants who have successfully completed a security check may work on cases within the jurisdiction of USKOK, while Article 13 (1) (4) of the Security Checks Act stipulates that persons working in specialized bodies for combating organized crime and corruption must undergo a basic security check. Similar provisions can be found in Article 99 (2) and Article 122 (3) of the State Attorney's Office Act for deputy state attorneys and for employees of the state attorney's office.

⁷² Wise consideration is needed regarding the catalogue of serious crimes whose prosecution would be possible based on evidence collected by security intelligence agencies, in order to avoid an excessive strengthening of their powers and the focus of the powers of security intelligence agencies on combating crime, which is not their task.

⁷³ See, *supra*, chapter. 5.2

⁷⁴ Declassification, or the release of intelligence agents from keeping secret everything they learned in the course of their duties for the purposes of criminal proceedings, cannot adequately protect national security, since it is illusory, not to say naive, to expect that defendants for serious crimes or even their lawyers, who may pose a security risk in the event of failure to conduct a prior security check in terms of acquaintances of intelligence personnel or the criminal underworld, will keep secret everything they learned during criminal proceedings or the investigation phase simply because they were warned to do so by the court or criminal prosecution authority.

equality of parties in taking procedural actions, which is again one of the aspects of the principle of equality of arms.⁷⁵

After the hearing, the court assesses the probative value of such evidence, the reliability of the evidence and the credibility of the witnesses.⁷⁶ Of course, the above includes amendments to several provisions of the Criminal Procedure Code, with an emphasis on the provisions on witnesses and the rules of the preparatory hearing, as well as the provisions on the confidentiality of data and proceedings. Jimeno Bulnes also emphasises that "the major risk here is a probable collision between intelligence information and/or reports and fundamental rights" and that "in terms of criminal procedure, the observance of such fundamental rights especially presupposes the protection of the principle of contradiction (or confrontation), jointly with the enforcement of procedural guarantees, and other defence rights."⁷⁷

It would also be advisable to consider expanding the catalogue of criminal offences under Article 187 (5) of the Criminal Procedure Code and to provide a normative path for establishing the identity of the defendant from personal data collected by intelligence agencies for criminal offences in the areas of, for example, organised crime, war crimes, crimes against humanity, genocide and cybercrime⁷⁸ committed against the state information infrastructure. In the context of the aforementioned article, it should also not be forgotten that there is a need to use clearer normative wording regarding the meaning of "exception" in order to

⁷⁵ Ivičević Karas, E., *Okrivljenikovo pravo da ispituje svjedoke optužbe u stadiju istrage kao važan aspekt načela jednakosti oružja stranaka u kaznenom postupku: u povodu presude Europskog suda za ljudska prava u predmetu Kovač protiv Hrvatske*, Hrvatski ljetopis za kazneno pravo i praksu, 14(2007), 2, p.1000.

⁷⁶ See more on this in: Vervaele J., *Posebne postupovne mjere i poštovanje ljudskih prava*, Hrvatski ljetopis za kazneno pravo i praksu, Vol. 16, No. 2, 2009, p. 951.

⁷⁷ Jimeno Bulnes, M., *op. cit.*, p. 190.

⁷⁸ With the entry into force of the Cybersecurity Act (Croatian: Zakon o kibernetičkoj sigurnosti, "Official Gazette" Nr. 14/24), the SOA becomes the central state body for cybersecurity, or rather its National Cybersecurity Centre, which, according to the narrative of its multidisciplinary work, will certainly obtain operational knowledge about the commission of criminal offences in the field of cybersecurity, and in this sense, its knowledge in this area will also be a valuable source of knowledge for criminal prosecution bodies that do not have as many capacities to fight technologically sophisticated crime and evidence is not easily available through classic investigative actions. Article 59 (1) (4) of the aforementioned Act provides that the bodies responsible for implementing cybersecurity requirements closely cooperate and exchange information with criminal prosecution bodies when incidents are the result of criminal activities, which additionally indicates the great importance of the SOA in particular in the analysis of security incidents that are often the result of the commission of criminal offences in the field of cybercrime. See more about this in: Kuzior, A.; Tiutiunyk, I.; Zielińska, A.; Kelemen, R., *Cybersecurity and cybercrime: Current trends and threats*, Journal of International Studies, 17(2), 2024, pp. 220-239.

reduce the possibility of different interpretations, and in this regard, the legislator needs to more clearly state, for the purposes of legal certainty, which are the exceptional situations when intelligence agency data can be used to establish the identity of the defendant, as stated above.⁷⁹

7. CONCLUSION

The issue of using intelligence data in criminal proceedings represents a point of contact between the work of intelligence agencies and law enforcement agencies. From this meeting of the two bodies, and taking into account their structure and the objective and legal possibilities for collecting information, law enforcement agencies could certainly benefit more if they used data collected by intelligence services. The hypotheses set out at the beginning are proven by the analysis in the paper. In the sections dealing with the organization of intelligence services and lesser legal restrictions on data collection, it was determined that the collection of data on perpetrators of certain criminal acts that also threaten national security is significantly less demanding for intelligence agencies compared to criminal prosecution bodies. Furthermore, a detailed analysis of legal provisions, primarily the Croatian Criminal Procedure Act, determined that the existing legal regulations should be interpreted in such a way that the use of intelligence services' knowledge as evidence in criminal proceedings is only exceptionally possible, based on the express provision of Art. 187 (5).

One of the main obstacles to such cooperation is the general reluctance of intelligence agencies to share their sources of knowledge with criminal prosecution authorities and thus reveal their informants, methods of operation and data collection. Compared to the main goal, which is to preserve their own capacities for the long-term preservation of national security, intelligence agencies consider information assistance in proving criminal proceedings through evidence presented contradictory to the hearing as a secondary goal, which is abandoned if it jeopardizes the primary goal.

If there is such willingness to share information and sources as evidence in criminal procedure, there is no doubt that cooperation between intelligence agencies and criminal justice can provide great benefits to law enforcement agencies, but the sensitivity of this issue cannot be emphasized enough since, as Vervaele warns, "it clearly emerges that the use of intelligence in the administration of criminal justice touches upon the foundations of a fair trial".⁸⁰ It

⁷⁹ See *supra*, chapter 4.

⁸⁰ Vervaele, J. A. E., *op. cit.* note 59. p. 439.

is not ruled out that in the near future the Croatian legislator, pressured by the increasing difficulties that criminal prosecution authorities have in detecting and proving certain forms of serious crimes that also threaten national security, will decide, like some other European countries, to "liberalize" the possibility of using intelligence data in criminal proceedings. As we can conclude from brief comparative law analysis presented in the text, such changes stand in the way of a whole series of things, namely the principle of adversarial justice and the principle of fair procedure in general, with a special emphasis on the right of the defense to question prosecution witnesses. Therefore, such legislative changes would eventually be acceptable only if the procedure for entering them into the evidentiary material was set up in a way that would not harm the fairness of the procedure and the rights of the defense. Some of such possibilities, modelled after some comparative systems, are presented in the paper. Taking into consideration the above mentioned, it can be said, as Manget F. observed, that the interaction between intelligence and criminal law can result in spectacular mountains and valleys, although sometimes there can be occasional earthquake or volcano between the two.⁸¹

REFERENCES

BOOKS AND ARTICLES

1. Arslan, C., *Intelligence in Criminal Procedure Law*, 2013/2, Ankara Bar Review, pp. 49-64.
2. Badžim J., *Obavještajna država tijela i kriminalitet*, Split, 2014.
3. Burić, Z. et al, *Upotrebljivost rezultata masovnog nadzora komunikacija kao dokaza u hrvatskom kaznenom postupku – slučaj SKY ECC*, Hrvatski ljetopis za kaznene znanosti i praksu, Vol. 30, No.2, 2023., pp. 243-274.
4. Čukljaš, Đ., *Tajno komuniciranje špijuna*, Ministarstvo unutarnjih poslova, Zagreb, 1994.
5. Damaška, M., *Dokazno pravo u kaznenom postupku: oris novih tendencija*, Pravni fakultet u Zagrebu, 2001.
6. Đurđević, Z., *Admissibility of evidence, judicial review of the actions of the European public prosecutor's office and the protection of fundamental rights, Protecting fundamental and procedural rights from the investigations of OLAF to the future EPPO* / edited by Valentina Bazzocchi, 2014, pp. 123-128.
7. Eijkman, Q.; Van Ginkel, B., *Compatible or incompatible intelligence and human rights in terrorist trials*, Amsterdam Law Forum, 3(4), 2011, pp. 3-16.

⁸¹ Manget F., *Intelligence and the Criminal Law System*, Stanford Law & Policy Review Vol. 17, 2006, p. 415.

8. Garačić, A.; Novosel, D., *Zakon o kaznenom postupku u sudskoj praksi I. i II. dio*, Libertin naklada, Rijeka, 2018.
9. Grubač, M., *Krivično procesno pravo*, Pravni Fakultet univerziteta Union u Beogradu, Beograd, 2008.
10. Hasanovic A. et al, *Nacionalna sigurnost Republike Hrvatske u 21. stoljeću – knjiga 2*, Jesenski i Turk, Zagreb, 2023.
11. Ivičević Karas, E., *Okrivljenikovo pravo da ispituje svjedoke optužbe u stadiju istrage kao važan aspekt načela jednakosti oružja stranaka u kaznenom postupku: u povodu presude Europskog suda za ljudska prava u predmetu Kovač protiv Hrvatske*, Hrvatski ljetopis za kazneno pravo i praksu, 14(2007), 2, pp. 999-1018.
12. Jenkins, D., *There and Back Again: The Strange Journey of Special Advocates and Comparative Law Methodology*, Columbia Human Rights Law Review, 42, 2011, pp. 279-355.
13. Jimeno Bulnes, M., *The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama*, New Journal of European Criminal Law, 8(2), 2017, pp.171-191.
14. Karas Ž., *Uvod u kriminalistiku*, Ministarstvo unutarnjih poslova, Zagreb, 2012.
15. Krapac D. et al., *Kazneno procesno pravo, Prva knjiga: institucije*, Narodne Novine, Zagreb, 2015.
16. Krapac, D. et al., *Kazneno procesno pravo, Prva knjiga: institucije*, Narodne novine, Zagreb, 2020.
17. Kuzior, A.; Tiutiunyk, I.; Zielińska, A.; Kelemen, R., *Cybersecurity and cybercrime: Current trends and threats*. Journal of International Studies, 17(2), 2024, pp. 220 -239.
18. Lalović D., *Suverena država – temeljni pravopolitički projekt moderne (2)*, Politička misao, Vol. XLII, No.3, 2005, pp. 33-49.
19. Malnar D., *Sigurnosno obavještajne studije*, Jesenski i Turk, 2024.
20. Manget F., *Intelligence and the Criminal Law System*, Stanford Law & Policy Review Vol. 17, 2006, pp. 415.-436.
21. Potparić D.; Veić P., *Uporaba proaktivne kriminalističke obavještajne djelatnosti u borbi protiv teških kaznenih djela i organiziranog kriminaliteta*, Policija i sigurnost, Vol 29, No. 4, Zagreb, 2020, pp. 356 – 375.
22. Tuđman, M.; Akrap, G.; Matošić, V., *Leksikon izvještajnog nazivlja*, National Security and the Future, 1-2 (22) 2021.
23. Vaško, A., *Intelligence information within criminal proceedings*, DANUBE: Law, Economics and Social Issues Review, ISSN 1804-8285, De Gruyter, Warsaw, Vol. 10, Iss. 3, 2019, pp. 267-283.
24. Vervaele, J. A. E., *Posebne postupovne mjere i poštovanje ljudskih prava*, Hrvatski ljetopis za kazneno pravo i praksu, Vol. 16, No. 2, 2009, pp. 913-961.

25. Vervaele, J. A. E., *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?*, International Review of Penal Law, Vol. 76, pp. 409-443.
26. Vogel, B., *Secret Evidence in Criminal Proceedings*, Max Planck Institut für ausländisches und internationales Strafrecht, Duncker & Humblot, Berlin, 2021.
27. Waxman, C. M.; Barak Erez D., *Secret Evidence and the Due Process of Terrorist Detentions*, Columbia Journal of Transnational Law, 3, 2009, pp. 3-58.

LEGAL ACTS

1. Act on the Security-Intelligence System of the Republic of Croatia, Official Gazette, No. 79/2006, 105/2006.
2. Courts Act, Official Gazette No. 28/2013, 33/2015, 82/2015, 82/2016, 67/2018, 126/2019, 130/2020, 21/2022, 60/2022, 16/2023, 155/2023, 36/2024.
3. Criminal Code, Official Gazette, No. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022, 114/2023, 36/2024.
4. Criminal Procedure Act of the Republic of Croatia, Official Gazette, No. 152/2008, 76/2009, 80/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017, 126/2019, 126/2019, 80/2022, 36/2024.
5. Cybersecurity Act, "Official Gazette" Nr. 14/24.
6. Data Secrecy Act, Official Gazette No. 79/07, 86/12.
7. Justice and Security Act of 2013, available at: <https://www.legislation.gov.uk/ukpga/2013/18/section/9>.
8. Police Duties and Powers Act, Gazette No. 76/2009, 92/2014, 70/2019.
9. Regulation on the content, appearance, filling in and handling of the Security Vetting Questionnaire, Official Gazette, No. 114/2008.
10. Regulation on information security measures, Official Gazette No. 46/2008.
11. Rulebook on the manner of acting of police officers, Official Gazette No. 20/2022, 37/2023, 114/2023.
12. Security Vetting Act, Official Gazette, No. 85/2008, 86/2012; Data Secrecy Act, Official Gazette, No. 79/2007, 86/2012.
13. State Attorney's Office Act, Official Gazette No. 67/2018, 21/2022.
14. The Police Duties and Powers Act, Official Gazette No. 76/2009, 92/2014, 70/2019.

COURT DECISIONS

1. I Kž-Us 22/11-11 of 8 February 2012.
2. I Kž 705/2008-5 of 3. March 2010.

3. Chahal v. United Kingdom, App. No. 22414/93.

NETWORK RESOURCES

1. https://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/2016/I_Degree_Security_Vetting_Questionnaire.pdf
2. <https://www.soa.hr/files/file/Public-Report-2022-en.pdf>
3. <https://www.otc.hr/>

OTHER SOURCES

1. Council of the European Union - Final report on the Evaluation of National Anti-Terrorist Arrangements, 18th November 2005, available online via: https://www.eumonitor.eu/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vi3aoj3pl4xq/f=/blg6836.pdf.