NAUKA I DRUŠTVO – SCIENCE AND SOCIETY
Časopis za društvene nauke – Journal of Social Science

God. 2021, Vol. VIII, Br. 1 (1-33)

Original Paper
UDC: 351.76.3(497.11).
DOI: https://doi.org/10.5281/zenodo.5519631
Received: 12 April 2021
Accepted: 27 April 2021

Zvonimir IVANOVIĆ*
University of Criminal Investigation and Police Studies Belgrade

Mina ZIROJEVIĆ
Institute of comparative law, Belgrade

FUNCTIONALITY OF THE ANITA PLATFORM IN THE LEGAL SYSTEM OF THE REPUBLIC OF SERBIA

Abstract

Back in 2018, the University of Criminal Investigation and Police Studies entered its first Horizon 2020 project with 16 other partners from a total of 11 countries as an organization that trains members of the police in the Republic of Serbia. The project itself presents a unique undertaking in the EU and beyond. It is intended to be an exploration-oriented form of an online platform for searching the deep, surface, and dark internet to obtain data on the objects, connections between subjects and prove their relationships and activities. This platform is a unique tool in the fight against illegal trade of narcotics, new psychoactive substances, as well as counterfeit drugs, weapons, and ammunition, as well as terrorist financing. The presentation of the possibilities of this platform is integrated with the approach to the analysis of possible measures and actions that would come into consideration for application in the legal system of the Republic of Serbia. Regardless of the way in which this well as proposals regarding possible procedural actions that are in the option for enforcing. In addition to showing the specifics of the platform itself and the platform is analysed and, although it is a tool applicable in the systems of EU member states, it is necessary to recognize its

E-mail: zvonko31@gmail.com.

usability in the legal system of the Republic of Serbia. To this end, in the Art. is presented an analysis of possible legal bases for action in the application of ANITA platform tools, astools that come with the work, it also offers an elaboration of the positioning of this tool in the legal framework of our country. although it is a tool applicable in the systems of EU member states, it is necessary to recognize its usability in the legal system of the Republic of Serbia. To this end, an analysis of possible legal grounds for action in the enforcing of ANITA platform tools is provided, as well as proposals regarding possible procedural actions that are in the option for enforcing. In addition to showing the specifics of the platform itself and the tools that came with the project, Art. also offers an elaboration of the positioning of this tool in the legal framework of our country.

Keywords: *Anita project, procedural measures, special evidentiary actions, OSINT, illegal trade*

INTRODUCTION

The combat against crime takes place in all available fields, and in that sense, any new methods and means are more than welcome, especially in the field of Internet searches. Our state, and the state's responses to crime, literally, in most cases lags the richer states and, for example member states of the European Union. European Commission projects related to scientific research contributions to society and communities with a huge budget range are not only reserved for member states but are also available to other states. We are lucky that within the Horizon 2020 call of the order of projects in the field of fight against crime and terrorism (FCT) and our state and institution, the University of Criminal Investigation and Police Studies (KPU) has connected with exceptional partners in order to create tools in the fight against organized crime and its incarnations on three levels of the Internet - superficial, deep and dark. This form of tool is a novelty in the region of our region, but unlike previous cases, this time we have access to the most modern type of tool through this form of cooperation with the privilege to be the first to try it and offer it to potential users in our market and environment.

THE SITUATION IN THE LEGAL SYSTEM OF THE REPUBLIC OF SERBIA

To understand to what (evidentiary) actions could be used tools available within the ANITAplatform, it is necessary to explain the current situation and available actions in the procedural - legal system of the Republic of Serbia. Criminal (conditionally speaking and procedural evidentiary) actions in the doctrine are divided into operative, evidentiary, and special evidentiary. This division is based on the division, conditionally speaking, provided by the Criminal Procedure Code (Art. 286). When solving a criminal offense and discovering the perpetrator, and during the formal and unformal activities of procedure, for the acting agency (whether it is the police, public prosecutor, or other agency), they require a legal basis for undertaking. The characteristic of any lawful and harmonized with criminal rules action of authorized police officers is reflected in the necessity of the simultaneous existence of a material precondition and a formal basis[1]. The material precondition is the existence of a criminal offense for which he is prosecuted *ex officio*, actually the certain level of suspicion that such a criminal offense was committed and that a certain person(s) committed the criminal offense (in special evidentiary actions the range of criminal offenses for which the material condition it is less binding - Art. 162 of the Code of Criminal Procedure is prescribed, and thus the circle of perpetrators targeted by these actions is reduced). The formal (criminal procedure) basis for criminal measures and actions taken by the police are certain provisions of the CPC and, possibly, certain activities of procedural subjects or their presence (proposal of the public prosecutorfor issuing an order for search or, for example, the presence of a defence counsel during the interrogation of the suspect by the police). When taking action, the acting agency has the obligation to take action in order to clarify the crime and apprehend the perpetrator, as well as to take the necessary measures to

[1] Ivanović Z. (2016). Dokazne radnje u digitalnom okruženju – kriminalistička analiza, Zbornik radova sa naučno-stručnog skupa sa međunarodnim učešćem *Evropske integracije:pravda, sloboda i ezbednost*, Tara, 24–26. maj 2016. (367-393). Kriminalističko-policijska akademija i Fondacija „Hans Zajdel", Beograd, p. 369.

find the perpetrator, in order to prevent hiding or escape of the perpetrator or accomplice, also, to discover and provide traces of the crime and acts and objects that may serve as evidence, and to collect all information that could be useful for the successful conduct of criminal proceedings. To fulfil this duty, the police according to Art. 286 of the CPC may take certain demand (operative) actions. These include the following actions: to request the necessary information from citizens; to carry out the necessary inspection and search of means of transport, passengers and luggage; to restrict movement in a certain area for the necessary time, up to eight hours at the latest; to take the necessary measures regarding the identification of persons and objects; to conduct a search in a form of an all point bulletin (APB) for the person and objects sought; to inspect certain facilities and premises of state bodies, companies, shops and other legal entities in the presence of the responsible person, to inspect their documentation and, if necessary, to confiscate it; to take other necessary measures and actions. A record or official note shall be drawn up on the facts and circumstances that were established during the enforcing of certain actions, and which may be of interest for the criminal procedure , as well as on the items that were found seized. This Art. envisages one in its essence and basis of sui generis

[2] Based on the initiative of police officers to the acting Basic or Senior Prosecutor for obtaining the realized telecommunication traffic of a natural person - ie retained data, the acting prosecutor submits to the pre-trial judge the initiative on the basis of which the pre-trial judge makes a decision to ask the communication providers to provide recorded information (retained data) on realized telephone communications, addresses of base stations or locate the address from which a certain communication was performed. Retained data represent information about the number being called, the number being called, the date and time, the start and end of the phone call, the duration of the phone call, the device used in communication, and the geographical location of the phone you are calling. a call has been made. Regarding the retention of data, we have a period of 12 months for their storage according to the Law on Electronic Communications. In the Law on Electronic Communications, as well as in the bylaws, which are to be adopted on its basis, as bylaws that more fully regulate their application, the rights and freedoms of man and citizen that are restricted are: guaranteed secrecy of letters and other means of communication in Art. 41 of the Constitution of the Republic of Serbia and guaranteed protection of privacy of personal data from Art. 42, as well as Art. 46 of the Constitution of Republic of Serbia in terms of freedom of opinion and expression.

action. According to the warrant (this is the only warrant existing in the CPC) of the pre -trial judge , and issued at the proposal of the public prosecutor , the police can obtain records of telephone communication , used base stations or locate the place from which communication is performed2. This action in the original form of the CPC was reserved for the Public Prosecutor , but due to the actual obstacles related to the supervision of communication and requesting a court decision , such a solution was subsequently found . The police shall immediately inform the public prosecutor about the undertaking of measures and actions , and no later than within 24 hours after the undertaking . A person against whom some of the measures and actions have been applied may file a complaint to the acting public prosecutor . The described actions can be taken by the public prosecutor at any time , but by the vocation , they are reserved for the police . Certain measures and actions are legally determined in the CPC, and their undertaking is conditioned, according to the conditions that must be fulfilled during the undertaking; they, as a rule, have probative value . According to the described , the conditions for taking evidentiary actions can be imperative or alternative . For the sake of illustration , we can cite the example of communicating a certain corpus of rights to a person who is deprived of liberty or a suspect who agreed to be questioned in the presence of defence counsel before the autopsy and exhumation . First of all, criminal -procedural evidentiary actions are provided exclusively by procedural legislation (CPC) and, as a rule, are regulated in detail only by this regulation (the elaboration of police actions in undertaking certain investigative actions is also contained in the Law on Police 6/2016, 24/2018-95, 87/2018-24) ZOP - for temporary seizure of items in Art.s 92, 93 and 94). Evidentiary actions are actions by which the agency in charge, in the conditions prescribed by law appears as the bearer of their implementation , as an authorized procedural entity entitled to take police, according to the rules of questioning the defendant (Art. Art. 68, paragraph 1, items 1 and 2 and Art. 69 of the CPC). If the conditions prescribed in this way are not formally fulfilled, the action taken and the results of its undertaking will not have a legally perfect effect - moreover, all records must be separated in a special envelope and excluded from the case file in a further trial. Evidentiary actions must be taken by the agency in charge, first, the head of the pre- investigation procedure and investigation - the public prosecutor and he (or she) may entrust the performance of these actions to the police, except for such action with the aim of producing legal consequences - the presentation of evidence in the procedure. As a rule, evidentiary actions (investigative actions) are performed by the public prosecutor, and in the law, especially in cases provided for, by authorized police officials (temporary seizure of objects, reconstruction of events,

[3] For criminal offenses for which a special law stipulates that the public prosecutor's office of special jurisdiction shall act (Art. 162, Art. 1, paragraph 1 of the CPC); as well as for the acts listed in Art. 162 par. 1 point 2, ie. aggravated murder (Art. 114 of the Criminal Code), kidnapping (Art. 134 of the Criminal Code), showing, obtaining and possessing pornographic material and exploiting a minor for pornography (Art. 185, paragraphs 2 and 3 of the Criminal Code), robbery (Art. 206, paragraphs 2 and 3 of the Criminal Code), extortion (Art. 214, paragraph 4 of the Criminal Code), abuse of position of a responsible person (Art. 227 of the Criminal Code), abuse in connection with public procurement (Art. 228 of the Criminal Code), receiving bribes in performing economic activities (Art. 230 of the Criminal Code), giving bribes in performing economic activities (Art. 231 of the Criminal Code), counterfeit- ing money (Art. 241, paragraphs 1 to 3 of the Criminal Code), money laundering 245, paragraphs 1 to 4 of the Criminal Code), unauthorized production and distribution of narcotics (Article 246, paragraphs 1 to 4 of the Criminal Code), endangering independence (Art. 305 of the Criminal Code), endangering the territorial integrity Art. 307 of the Criminal Code), attack on the constitutional order (Art. 308 of the Criminal Code), calling for a violent change of the constitutional order (Art. 309 of the Criminal Code), diversion (Art. 313 of the Crimi- nal Code), sabotage (Art. 314 of the Criminal Code), espionage (Art. 315 of the Criminal Code), disclosure of a state secret (Art. 316 of the Criminal Code), incitement to national, racial and religious hatred and intolerance (Art. 317 of the Criminal Code), violation of territorial sovereignty (Art. 318 of the Criminal Code), association for unconstitutional activities (Art. 319 of the Criminal Code), preparation of acts against the constitutional order and security of Serbia (Art. 320 of the Criminal Code), serious acts against the constitutional order and security of Serbia (Art. 321 of the Criminal Code), illicit production, possession, carrying and trafficking of weapons and explosives (Art. 348, paragraph 3 of the Criminal Code), illegal crossing of the state border and smuggling of people (Art. 350 para. 2 and 3 of the Criminal Code), abuse of official position (Art. 359 of the Criminal Code), trading in influence (Art. 366 of the Criminal Code), accepting bribes (Art. 367 of the Criminal Code), giving bribes (Art. 368 of the Criminal Code), trafficking in human beings (Art. 388 of the Criminal Code), endangering persons under international protection (Art. 392 of the Criminal Code) and a criminal offense under Art. 98 para. 2 to 5 of the Law on Data Secrecy.

investigation and expertise, interrogationof suspects, search, confrontation and identification). Under Chapter II of the CPC, the following actions are explicitly stated as evidentiary actions: search of an apartment and a person, search of the automated processors of digital data, temporary seizure of items, handling of suspicious items, examination of the defendant, examination of witnesses, CSI investigation, and expertise.

Special evidentiary actions may be ordered against a person for whom there are grounds for suspicion that he has committed a criminal offense under Art. 162 of the CPC, and otherwise evidence for criminal prosecution could not be collected or their collection would be significantly hindered, under the conditions of Art. 161 CPC. Special evidentiary actions may exceptionally be ordered against a person for whom there are grounds for suspicion that he is preparing any of the criminal offenses referred to in paragraph 1 of Art. 162[3], and the circumstances of the case indicate that the crime could not have been detected, prevented, or proved in any other way, or that it would have caused disproportionate difficulties or great danger. When deciding on the determination and duration of special evidentiary actions, the acting agency will especially assess whether the same result could be achieved in a way that less restricts the rights of citizens. In the Chapter VII, Part 3 of the CPC, are prescribed measures of the prosecuting authorities for the detection and proving of criminal offenses from Art. 162 of the CPC, and they are there also envisaged, and determined as special evidentiary actions (formerly called special investigative measures). In terms they are: secret surveillance of communication (Art.s 166-170); covert surveillance and recording (Art.s 171–173) simulated jobs (Art.s 174–177); controlled delivery (Art.s 181– 182) and computer data retrieval (Art.s 178–180). As a special, specific, action of the prosecuting authority for the detection and proof of criminal offenses under Art. 162, para. 1, point 1 of the CPC (for which , according to special laws , prosecutor 's offices have special competencies), the legislator also foresaw the engagement of an undercover investigator (183– 187). The action of an undercover investigator can be determined only for criminal offenses within the competence of special prosecutor 's offices . It is important to emphasize here that these actions can be undertaken and that their results can have probative value only if they are undertaken against certain persons (suspects for acts under Art. 162) as well as in connection with criminal offenses provided for in Art. 162 of the CPC. para.1. point.2. A special evidentiary action under Art. 183 of the CPC (PI) may be ordered only for a criminal offense under Art. 162 st. 1 item 1. Under the conditions from Art. 161 of the CPC, a special evidentiary action from Art. 166 of the CPC (secret surveillance of communication) may be ordered for the following criminal offenses: unauthorized use of a copyright work or subject of related law (Art. 199 CC), damage to computer data and programs (Art. 298 para. 3 CC), computer sabotage (Art. 299 CC), computer fraud (Art. 301 para 3 CC) and unauthorized access to a protected computer , computer network and electronic data processing (Art. 302 CC). So, special evidentiary actions may be undertaken only in connection with criminal offenses provided for in the CPC (Art. 162), by persons authorized to undertake such actions (determined and provided for by special laws). A special evidentiary action (PDR) of interest for this work is computer data retrieval . It was defined differently during its development as an automatic computer search of personal and other related data to have this name today. From this second form of the name, one can conclude about the logic and essence of the action. A special evidentiary action is provided for in Art. 178-180. ZKP.The conditions for the possibility of application are, as with any other special evidentiary action, the basic conditions provided by the CPC. Computer search of personal and other related data and their electronic processing (in the form of comparison) may be undertaken if there are grounds for suspicion that a criminal offense referred to in Art. 162, paragraph 1, item 1 and 2 of the CPC, if evidence for criminal prosecution cannot be collected in any other way or their collection would be significantly more difficult. The measure consists in a computer search of already stored personal and other, directly related data and in their automatic comparison with the data related to the criminal offense under Art. 162. para.1 point 1 and 2 of the CPC and the suspect. This seems to exclude as possible suspects persons in respect of whom it is unlikely that they relate to the crime. Of course, the same cannot be the only reason for applying this measure. It carries with itself significant potential in terms of evidence and searching for such data and generating positive results of such a search can be very important evidence in the proceedings. The measure is ordered by the pre-trial judge, at the reasoned proposal of the public prosecutor. The order contains data on the suspect, the legal name of the criminal offense, a description of the data that needs to be searched and processed by computer, the designation of the state body that is obliged to search the requested data, the scope and duration of the special evidentiary action. The measure can be enforced for a maximum of three months, and due to the necessity of further collection of evidence, it can be exceptionally extended for a maximum of two more times, lasting three months each. The computer search of data is to be stopped as soon as the reasons for its enforcement cease (the total duration of the measure is nine months). The measure is implemented by the ministry of internal affairs , BIA , VBA , customs services , or other state agencies , that is, other legal entities that exercise certain public powers based on the law . The purpose of applying this action , therefore , is related to computer search of data collected and stored in some databases or in generating a database and obtaining hits on keywords or search objects that are predefined for the purposes of applying this PDR.

Procedure for application The order contains data on the suspect, the legal title of the criminal offense, a description of the data that needs to be searched and processed by computer, the designation of the state body that is obliged to search the requested data, the scope and duration of special evidence . Upon completion of the computer data search , the agency or legal entity submits to the pre-trial judge a report containing:

data on the start and end time of the computer data search, data searched and processed, data on the official who conducted the special evidentiary action, description of the applied technical means, data on the persons involved and the results of the applied computer data search. The pre-trial judge will submit this report to the public prosecutor. If, by undertaking special evidentiary actions, material on a criminal offense or perpetrator was collected that was not covered by the decision on determining special evidentiary actions, such material may be used in the procedure only if it refers to a criminal offense under Art. 162 of the CPC. Special registers are formed on the undertaken actions. Such a proposal for determining special evidentiary actions and decisions on the proposal shall be recorded in a special register and kept together with the material on the conduct of special evidentiary actions in a special envelope, with the indication "special evidentiary action" and the degree of secrecy, in accordance with regulations related to classified information. Information on proposing, deciding, and conducting special evidentiary actions is classified information. They are obliged to keep them as secrets and other persons who find out about them in any capacity. If the public prosecutor does not initiate criminal proceedings within six months from the day when he became acquainted with the material collected through the use of special evidence or if he states that he will not use it in the proceedings, ie that he will not request proceedings against the suspect, the pre-trial judge will issue a decision on the destruction of the collected material. The procedure related to the notification of the persons who were the subject of the action taken under Art. 166 is specifically prescribed by CPC. The pre-trial judge may inform the person against whom the special evidentiary action referred to in Art. 166 of this Code was conducted if the identity was established during the conduct of the action and if that would not jeopardize the possibility of conducting criminal proceedings. The material is destroyed under the supervision of the pre-trial judge, who draws up a record of it. If during the undertaking of special evidentiary actions, it was done contrary to the provisions of this Code or the order of the agency in charge, a court decision cannot be based on the collected data, and the collected material is handled in accordance with Art. 84, paragraph 3 of CPC.

OSINT

In the framework of the consideration of operative actions, it should be noted that although they are named in the CPC, ZOP, and some other regulations, they are still not fully enumerated, nor fully prescribed. These include the so-called. OSINT which, in addition to special evidentiary actions, is important for this work of ours. Open-source intelligence (OSINT) technique involves collecting data from the so-called open, publicly available sources, in order to use them for intelligence purposes. There is no precise date when the term OSINT first appeared, however, as a relative term it has probably been used for hundreds of years to describe the act of gathering intelligence using publicly available resources. In recent history, OSINT was introduced during World War II as an intelligence tool by many security services, but with the extensive growth of Internet communications and the vast amount of digital data produced by the public around the world, OSINT is now becoming a necessity for various organizations. In this sense, government services, non- governmental organizations (NGOs) and business corporations are beginning to rely more on OSINT rather than private and classified data. OSINT sources differ from other forms of intelligence in a manner that they must be legally available to the public, without violating constitutional norms, which relate to guaranteed rights and freedoms, primarily the right to privacy, the right to protection of personal and family home, freedom of communication but also copyright and related rights. This difference makes the possibility of collecting OSINT sources applicable in different spheres, not just security. For example, companies may benefit from using these resources to gain knowledge about their competitors without violating the rules of unfair competition and economic shipowners through such activities . The United States Department of Defense defines OSINT as "the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement”[4] and not just security. For example, companies may benefit from using these resources to gain knowledge about their competitors without violating the rules of unfair competition and economic shipowners through such activities. For example, companies may benefit from using these resources to gain knowledge about their competitors without violating the rules of unfair competition and economic shipowners through such activities.

Social networks open numerous opportunities to collect data and support investigations of any kind due to the huge amount of useful information, which can be found in one place. For example, a large amount of personal information about any person around the world can be obtained by finding only that person's Facebook account, if it is not false or intentionally altered, in order to place misdirected information. In addition to being of great importance to the intelligence community, OSINT collection is cheaper and less risky than traditional data collection methods, because all it takes to collect data from OSINT resources is a computer, an Internet connection, and adequate expertise. As stated, the amount of data and the intensity of communication that takes place over the Internet is growing rapidly, and therefore their search is difficult. For example, the statistics of the YouTube platform show that about 300 hours of video material are published every minute, while the social network Facebook at the time of writing this paper has about 2.5 billion active users and 83 million fake accounts. It happens that when searching public sources, confidential data is found that are not adequately protected . Such "leaked " data can be e.g. found on websites such as WikiLeaks. Paradoxically, although confidential and collected illegally,

[4] Headquarters, Department of the Army (2012). Open-Source Intelligence, *Army Techniques Publication* No. 2-22.9 (FMI 2-22.9). Available at https://irp.fas.org/doddir/army/atp2-22-9.pdf (31.3.2021).

such data have become suitable for the OSINT method of data collection by the fact that they have become publicly available. Notwithstanding such facts, according to the rules of criminal procedural law in Serbia, the data obtained in this way cannot be used as valid to provide evidence in the proceedings but can be examined as such. Their usefulness is limited to operational activities. According to the 2001 NATO Handbook on Data Collection from Public Sources, there are four categories of data that can be obtained from public sources:

• Generic data from primary sources, such as photographs, audio and video material, satellite photographs, databases, metadata, etc .; • Generic data that has undergone a specific processing and filtration process to meet certain criteria or needs, such as. books that cover certain topics, Art.s, dissertations, journals, technical reports, internal documents of commercial companies, as well as other contents that have been processed by their creators. They are also called “Gray literature” because they are published outside traditional and academic distribution channels; • Data from public sources that have been converted into information that has been disclosed, processed and intended to meet certain criteria and needs in the broadest sense; • Confirmed data from public sources, which have a high degree of accuracy and which are confirmed by other sources that are not public, or data from reliable and respectable public sources. They are of particular importance, as there may be intentionalpublic disclosure of inaccurate data to interfere with OSINT analysis. As OSINT includes all publicly available sources, including those on and off the Internet, such sources can be divided into four groups: • Internet (forums, blogs, social networks, video platforms, search platforms for individuals and legal entities, registered domains and IP addresses, geolocation data, as well as everything else that can be found online that will be the subject of basic processing of this paper); • Traditional mass media (radio, television, newspapers, books and magazines); • Specialized journals, academic publications, dissertations, annual reports of companies ; • Photos and videos including metadata • Geospatial information (e.g. commercial maps and cartographies).

Today, as we live in the information age, publishers, corporations, universities and other actors are shifting their business processes to digital form. Also, the number of social network users will continue to increase, as will the number of "Internet of Things", which will lead to a huge increase in the amount of digital data coming from a large number of sensors and machines, making primary online data sources for OSINT analysis in the future.

ANITA PROJECT AND GOALS

The basis of the project is the ANITA platform for the application of several different tools that are modularly incorporated into a system that uses the latest scientific advances and cutting-edge technologies in order to achieve efficient analytical and collection activities on surface, deep and dark Net (Surface, Deep and Dark Net). These tools are independent, although they are integrated into a platform that, in addition to phenomenological analysis, performs other analyses and provides the system user with a comprehensive resultant with the possibility of its interaction in order to direct analytical tools and results that the system offers after applying analytical and other tools. The meaning of the system and its sustainability, as well as its applicability are defined in three basic scenarios - New psychoactive substances, counterfeit drugs and narcotics, Weapons (firearms) and ammunition and terrorist financing primarily through cryptocurrencies. Illegal trade takes place on all three levels - surface, deep and dark internet - network. The premise of the ANITA platform and the tools it uses is based on compre hensive analysis of consortium members in which, for example, an analysis of 6 markets on the darknet in the period 2016-2018 was performed[5] regarding heroin, cocaine, specifically the analysis of all drug market markets. Also then was performed the specialized analysis of the market of cannabis, tobacco and new psychoactive substances, as well as the

[5] Analysis for DNT project, available at: www.dntproject.eu (31.3.2021).

general criminological analysis. As a result of the analysis, various forms of conclusions are offered about the relations of criminal groups that distribute narcotics, ways of their distribution, creation of new ways and means of distribution and profiling of sellers in dark net markets, the origin of classical narcotics in relation to new psychoactive substances. In terms of additional analysis , a parallel can be made with the second scenario regarding weapons and ammunition , where narcotics and weapons and ammunition are very often imported. The criminological as well as scientific - professional basis of the platform and its functionality are the analysis of online illicit forms of trade and the study of strategies and measures in counteracting such phenomena. Specifically, the analysis covers activities, processes, trends and human factors that affect online trafficking , all with the aim of raising awareness of key actors (in example law enforcement) about potential risks as well as providing first -hand knowledge with sets of recommendations on effective countermeasures that are to be undertaken in the fight against such phenomena . The goal is for the platform to be a living organism , which receives guidance on the undertaken activities and training and fine-tuning from the participants in the construction of the project, members of the police units involved in the project and the security advisory board. This includes both the evolution of the phenomena observed and the updating of the actions of the prosecuting authorities through operational advice and guidance from police units.

The procedures underlying the system are on the one hand real phenomena that have their moment of evolution and on the other hand operational guidelines that the technical part of the project consortium must turn into an operational functional platform with adequate and fully integrated tools. Observing the evolution of the problem includes analysis of actors at all three levels of the network, their measures in order to hide their identities and actions in the markets, while operational guidelines provide the following analysis. In the field of surface network - surface net nicknames of sellers, “stores” that sell and advertise certain new psychoactive substances (NPS), online pages of doctors and pharmacies (pharmaceutical companies), direct ads on social media, video sharing with narcotics, do it yourself videos about narcotics, videos that of sellers, direct advertising, instructions on how to get in touch with sellers, gain access to certain markets, forums dedicated to drug trafficking, video sharing with drug topics, forums dedicated to drug quality assessment and other narcotics related forms of services. In the domain of the hate network-dark net, sellers nicknames, street names and titles, as well as famous brands, user feedback - feedback, search engines - grams, torch, discussion forums (DREAD/HUB FORUM). Through the analysis conducted within the ANITA project, a classification was made into two groups of markets for illicit products on the dark net: crypto markets and dealer stores[6]. Based on the analysis, the classification and payment methods through the main virtual currencies in crypto -markets – until recently , most often Bitcoin , and increasingly Monero and Etereum , but also traditional currencies that have recently appeared on the dark net. The communication channels provided by the analysis appear in the following forms , encrypted applications , most often used among sellers , dealers and buyers in order to avoid surveillance, the use of instant messengers with automatically generated and temporary identities using Surespot app, Wickr , KIK, Tails and the like. The analysis also yielded results according to which the social media vector in advertising is extremely important (Facebook) as well as the registered role of search services and spam to promote online commercialization of drugs.

Criminal strategies that should be used in prevention and suppression match criminal strategies, are defined through the analysis of the latter. In dark net markets, exit fraud strategies have been recognized, phishing (by which sellers and manufacturers who offer their products warn users who do not need to follow the links posted on the ratings and pages for

[6] Compare with: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html (07.2.2021).

the evaluation of purchased illicit products), cases of non-delivery of goods, etc. Separately for each of the scenarios described in the earlier part of the text, evolutionary cycles and operational guidelines are developed. Each of the described scenarios has its realization most often through the forms of crypto-currencies, and the analysis of crypto wallets and realized transactions provides exceptional opportunities in the identification of participants in transactions[7]. It is important to point out that each of the network levels has its own form of connection with the previous one, and that the actors whose identifications are sought leave their information in the form of traces on them and can be tracked. In terms of communicating messages with advertising content, one should also understand the concept introduced by Brian Solis back in 2008 in the form of a conversational prism now at level 5.0, in which he tried to show observers in more detail to better understand, appreciate and understand the "status sphere" and its evolution through a still ongoing study in digital ethnography that follows dominant and promising social networks and organizes them according to the way they are used on a daily basis[8]. At the heart of this lie the teachings that look atthe everyday discourse of advertising through all three spheres of online illicit products. For each of the specific categories that we process within the ANITA platform, it is necessary to evaluate and evaluate the following main elements to more fully and in detail explore the ways in which the Internet transforms criminal modes of action - *modi operandi*.

They are:

- Specific role of surface, deep and dark net.
- Changes in the typologies of substances and products
- Legal status of substances of products as well as the legal environment that regulates the (mis)use of medical substances – drugs, precursors, New psychoactive substances – NPS

[7] For example: walletexplorer.com or poloniex.com. Specially designed tools. Graph Sense or Tag Sens – as a part of DANTE H2020 project – providing research of incoming and outcoming transactions and thus providing ideal support in investigation of these activities and their actors.

[8] https://www.hospitalitynet.org/opinion/4083995.html (31.3.2021).

- Risk in implementing regulations
- Availability and price of traditional medicines
- Geographical area of importance and relevant routes for smuggling
- Role of organized criminal groups and relevant criminal networks.

In analysing these activities, each of the scenarios can provide us with certain conclusions and the opportunity to implement them on the platform through the tools incorporated into it. Technically, they include several different system elements that will be discussed later. Some of them are a social model of raw materials or products themselves, models of distribution and concealment of the entire advertising process - advertising, making available illegal material,user evaluation of quality, functionality and purity of illicit products as well as sales or the entire transaction between seller (manufacturer) and buyer. Profiling the entire advertising process - advertising, making available illegal material, user evaluation of quality, functionality and purity of illicit products as well as sales or the entire transaction between seller (manufacturer) and buyer. Profiling according to the research of RISSC[9], which referred to 6 crypto markets, indicated the virtual origin of shipments, mostly the European continent and the North American continent, followed by Oceania and Asia in 2016, while in 2018. The survey achieves different results in Europe (51.8%), North America (16.5%), Asia (3.8%), and Oceania (2.9%). The rest are all others in the figure of 1%. The role of the partner institutions of the ANITA project was among other things, to more fully define the origins and destinations according to the operational knowledge of active sellers and buyers in the territories of the countries from which the police units within the ANITA project come. With this auxiliary tool orientation within the ANITA platform, there is a correction and fine-tuning of the sensor within ANITA.

ANITA PLATFORM AND TOOLS

The ANITA Platform is available at http://217.172.12.209:9090 and is a

[9] https://www.rissc.it/ (31.3.2021).

user interface that binds all forms of tools that will be displayed later and functionally connects the entire system. This platform is a form of tool that is an application for the management of investigative activities, and which allows the detection and reconstruction of a network of perpetrators of crimes in specific areas. Searching and retrieving data is the first step in processing on the platform. Data entry is based on several different sources - scrapping, that is, literally copying the dark net market to servers that provide their functionality and capacity to this system, as well as online search capabilities. In this phase, we are talking about the analysis of data sources and streams. In addition to such defined entries, we also have an overlay that translates the current surface net and other provided content (text to text, speech to text, speech to speech and text to speech) through the engagement of partner servers SYSTRAN[10], and allows all translations performed at the request of the user. The platform is offered at the initial level through the possibility of creating the role of administrator - investigation manager and assigning investigations to participants and another form - basic users, who can conduct investigations. Searches can be performed within the protected environment of the ANITA platform, but also on the surface internet. Once created, the investigation has more functionality, and is displayed on the graphical interface in the form of a network of connected , or partially connected entities. They appear in multiple functional forms, in the form of, for example, photographs , documents , functional connections , faces, videos or audio recordings . Each of the forms is interactive, predefined in the system with a special icon, and can be accessed with various forms of additional functionalities, depending on the processing of the system, functional connection with the creator, as well as access options defined by the system and protection . The platform provides opportunities to discover and monitor certain resources - defined as listening to the Internet. Capacities are also offered for the analysis of large amounts of data and analytical activities during

[10] https://translate.systran.net/ (31.3.2021).

analytics here. Within the graphical interface, there are various functions that enable further activities on the analysis, as well as assigning tasks to the system itself. Some tasks, such as crawling a particular website (complete digital acquisition), require additional time to perform such a task, and you should also take into account the workload of the system (it is literally copying the entire content of the website for which it is necessary to have enough server space, as well as free servers to perform these activities). The Home button allows you to return to the platform's home menu from where you can proceed further and again. It is possible to start a completely new investigation by entering the entities of interest and making additional connections, while assigning tasks to the system itself. The graphical interface can be changed to a list of active objects, but its display provides several significant advantages in recognizing connections and the possibility of additional influence on the analysis by the researcher himself. In any case, we have a presentation of simplified features and characteristics of a particular object of interest (description, type of object according to the annotation, title, presentation of the same - image, video for investigations - which is the identification element of the investigation, description, status of the investigation and which inspector active, etc.), in an additional window about the object (button About) as well as additional functionality about the annotation. During the research, it is possible to add a new object in one of the offered forms (source, location, object, transaction, web source, digital wallet, person, organization, event, and digital identity). Also available is a mouse pointer hovering mode that displays a simplified display of features. Each of the entities can be changed, most often this can be done by right-clicking on the object itself, and it is additionally possible to require the system to display more possible connections based on the algorithms existing in the system itself, and that object or node will be removed. In addition to this, there is an existing application button that introduces additional capacities of the platform itself and provides exceptional opportunities for further exploration of the entities. In the next step, within the applications, it is possible to perform an analysis of financial transactions with entities that enable it, so it is possible to search for a specific transaction in the available data, digital wallets, etc. Current exchange rate movements in the exchange of the most current cryptocurrencies are also provided. The next application is surveillance - which can instruct the system to monitor a particular source or resources, social media accounts, social media by type and for a particular object shape, entering keywords as well as the time in which the monitoring will be performed. The next application is deep web crawling (which involves downloading content with large amounts of data - which includes a wide variety of data) which is given tasks such as downloading the entire content of a darknet market. This is the most demanding application on the platform, and one should be careful when defining the tasks for it and the resources it will take up. Within the results, it is possible to see several different pages that include downloaded web pages, categories, URLs, as well as resellers. It is also possible to manage activities within this application, so it is possible to pause and stop downloading content, but within the obtained results it is also possible to add new categories - entities. The tools available in this application can also be linked to keywords and sources, with determination of the time range for crawling. In the case of applications, there is also a part related to the requested data or copies of data with the result of their request - rejected, accepted and the implementation is in progress. The capacity of the information extraction platform should also be pointed out, which may have probative value. After all, there is the possibility of creating and modelling intelligence that represents the current currency for all participants in the investigation, through the creation of standards and ontologies. Through machine learning, this platform promises both the possibility of classifying data and performing certain triage in terms of the usability of such data in the investigation. In general, this platform, in addition to the above, can be very good tool in assistance of investigations and decision-making in the operational processing and clarification of criminal offenses, but it can be used for evidence gathering and presering.

MODULES

In the next step, we will show the modules on which the ANITA platform is based, on which the tools within the system rest. The modules are divided into several different units: Investigation area, which includes investigation management, investigative graphic researcher, actions regarding requests for duplicate data, handling the chain of evidence and evidence in general, their export and import from and into the system; Surveillance of sources - surveillance task manager, dark net crawler, Twitter crawler, reddit crawler, surface internet crawler, blockchain analysis services, reconstruction of the source network, Tool for analysis of illegal trade trends; Photo and video analysis: object and concept detectors on photos and videos, visual indexing of places and weapons; Audio analysis tools: speech to text; Tools for the reconstruction of criminal networks, search and retrieval services in ANITA memory space, searches on external sources, extraction of evolving knowledge, validation of new and existing knowledge and intelligence, blockchain search engine and visual analytics; Unconscious human feedback incorporation into the platform, transfer of knowledge to new learners from the platform. We will explain some of these modules in more detail as follows.

Visual analysis module

As a functionality, it offers the provision of precise and time-efficient detection and recognition of high-level semantic concepts (objects, concepts, and events). The meaning and reasoning that encompasses or carries this module is related to the machine understanding and classification of specific entities that appear in a photograph or video. It also includes the detection and classification of people, activities, and objects. The purpose of the platform is to identify the different entities that appear on certain objects – scenes of photographs and videos, as well as the detection of specific concepts of importance.

Photo and video indexing module

Its basic functionality enables precise and time-efficient extraction of relevant content from large-scale databases. The specifics that adorn this module are the creation of short binary codes, after which it is possible to quickly extract videos and photos. In the platform system, the meaning and purpose of this module is to pull visually and semantically similar content according to the user's request (video frame).

Module: Object detection with improvement through the analysis of system user behaviour

Its basic functionality is enabling precise and time-efficient object detection with the use of a human perspective of visual recognition (recognition). This module attempts to incorporate artificial intelligence and machine learning through contextual specialized object detection with elaboration of expert experience. The system of this module is based on monitoring and analysis of human subjects - experts and their reactions during object recognition in order to create scientific and machine knowledge from these activities and incorporate it into the process of object detection in the system. A contribution to the overall ANITA system is the identification of the context of visual objects. Its basic functionality is enabling precise and time-efficient extraction of relevant content from databases.

Machine text translation module

This module enables the translation of multi-modal text content entries of the file type (office, Microsoft portable document format - PDF, Hyper Text Markup Language, hypertext markup language, XML Extensible Markup Language, or extensible (meta) markup language markup) of text documents, it is a standard set of rules for defining the format of data in electronic form) but also audio files (and those downloaded from video). Real-time translation of the desired content into selected languages within the REST application, which is a functional incorporated part of the ANITA platform. Translationis done in over 150 language combinations[11]. Translations are realized through the application of neural machine translation software solutions; it is a software-hardware construction of a system that learns independently and is constantly improved. The functional connection between the ANITA platform system and this module is reflected in enabling the user to view and understand the downloaded content even when it is not in the user's native language and includes the described language combinations. One of the modules related to this provides the possibilities of stylometric analysis, according to which one can conclude about the personality of the person who is the auto textual record being analysed, his education, personality characteristics, etc.

Speech-to-text translation module

This module offers the possibilities of multimodal translation services (text- to-text, speech-to-text, text-to-speech, and speech-to-speech) or, first, textual speech translation from related and compatible spoken and spoken sentences to text. Software hardware engines can vary depending on the domain and language pairs (from which it is translated to which) placed on the server that is currently on duty on the ANITA platform to which the user is connected. In terms of content, it is about translating audio content into text for further translation and analysis. The purpose of this module for the ANITA platform is to enable the researcher - police officer (inspector) to review and understand audio content that is not in his native language. Acquisition module with dark market crawler This module retrieves all data from deep net sites and dark net markets. The contribution of this module is exceptional in the field, primarily, of obtaining all materials from described sites, as well as fully documenting and providing covert services (including, files, photos, and video stimulation).

[11] Partner that is providing this application is SYSTRAN and this partner is adding that avail- able engines in translation (servers and software solutions) can in dependence of domains and language pairs that are deployed on the server dedicated for that particular moment for ANITA project integrated platform.

It is also important that such a tool can be used to conduct an investigation without the danger that the person conducting it will be noticed, as well as that the investigation can be noticed, and with the acceleration of actions, the general acceleration of the investigation. A special contribution of this module and tools is in the processing and analytical value of the data obtained from the market.

Darknet source identification crawler module

The module serves to identify possible sources, markets and communication channels through surface, deep and dark (dark) net. A special added value of this module is that the results of crawling (complete digital acquisitions) are not corrupted by search engines because they apply blacklists regarding criminal or prohibited activities. Fully suitable documentation and material for use in court, including photos, files, and streaming video files.

Human factor integration module in the analytical cycle

This module integrates user reactions, considering and integrating user attitudes, all to enable interaction with the system and improve the model of machine learning. The additional value of this module is that it enables automatic adaptation of the user interface and content, but also that it improves the robustness and performance of the detector of the desired measurements. The role in the ANITA platform system is to enable the use of system learning and independent improvement of the system as well as the transfer of knowledge for training new system users. This system uses several different sensors that monitor users and their reactions, based on which the system learns. The sensors are eye tracker, mouse activity, keyboard, and camera. The data collected by the sensors are pupil dilation, narrowing of the eyelids in the eyes, the quality and quantity of movements in the mouse, typing and content text in the keyboard sensor and facial expression in the camera. It is measured in the eyes - emotional state and cognitive load, quantity, and quality of movement in mice, affective state (excitement and valence) in the keyboard and emotional state in the camera. Based on these input factors, data is processed in the ANITA system, as well as data integration and analysis, followed by the creation of user modeling, enabled by artificial intelligence . Basically , the analysis concludes on the mental state of the user, physical and motor condition , physiological and in general mental , psychological state of the user and on that basis on the correct actions within the system. The goal is to improve the system in terms of decision-making and reasoning about the links and results of the analytical process within the ANITA system. Within the system itself, the following activities can be pointed out as an example . Personality intelligence can be obtained with the following tools: surface crawler, deep and dark web crawler, speech to text module, multilingual automatic translation, text analysis and stylometric analysis. E-mail data: multilingual automatic translation, text analysis and stylometric analysis, visual indexing, object detection and concept detection. Tasks related to markets on the dark net in the form of acquisition and analysis are obtained by crawlers of deep and dark network , reconstruction of the network by sources of multilingual automatic translation, text analysis, visual indexing, object detection and concept detection. Detection of crypto transactions through multilingual machine translation, text analysis and blockchain analysis. Analysis of connections between people and products through stylometric analysis, visual indexing, reconstruction of the criminal network, search and retrieval of data, extraction of evolving knowledge.

POSITIONING WITHIN THE LEGAL SYSTEM OF THE REPUBLIC OF SERBIA

Given the above, it is possible to recapitulate the same in relation to the ANITA platform. The presentation gave us an understanding of the available measures and actions in the procedural sense and criminal procedure in the Republic of Serbia. If we look at the meaning and goal of the introduction of PDR, according to the teleological interpretation, it is necessary to understand that these are actions that encroach on the freedoms and rights of man and citizen by the state apparatus in such a way that it is necessary to exercise multiple supervision. In that sense, the application is reserved as a rule for the police, the first level of supervision and control is with the head of the pre-investigation procedure - the competent public prosecutor's office, while the second level is within the jurisdiction of the pre-trial judge, who issues orders (for most PDR, except for controlled delivery) but also later when the files on the actions taken are submitted to him in order to forward them to the Prosecutor's Office. Search operations do not have these forms of control, especially when we look at OSINT. Our conclusion in the field of application of the ANITAplatform is that it requires in the part where searches are undertaken in the darknet (dark part of the network). Where certain persons appear with the intention of not establishing their identity - because the basic precondition for access to this area of non-indexed Internet is the use of the TOR browser, which by definition does not reveal the location or identity of the user but hides it through the TOR node network. Due to the described characteristics of the application of certain aspects of this platform, it is easy to treat it as a tool that encroaches on rights and freedoms in such a way that it is necessary to treat it as an action that belongs to the PDR. On the other hand, forensic standards, which are met by the platform in terms of preserving the chain of evidence and the technical background regarding the application of certain methods within the module, this tool meets the standards required by the PDR application framework. Of course, it is possible to consider aspects that would provide material so that we can consider and define within the evidence of actions. If we were to think about this option - of course it is also valid, but then we would not need additional judicial control or appointment by the court, but only the Public Prosecutor. Some spheres of application of this platform have a dimension that can be within the scope of even demand operations. It should be cut and given that we have already discussed the PDR in the first part. We believe that the application of the platform must require a reasoned form of initiative by the police or another body from the body of procedure - the In charge – acting Public Prosecutor, which would address a reasoned request to the competent judge for pre-trial proceedings in order to issue PDR. Of course, if both the search and the search areas could be limited to the public sphere and the superficial and deep internet where the data are publicly available, then something like that would not be necessary. The platform has such capabilities and it is possible to differentiate such requirements in the same way, it remains an additional "fine-tuning" of the platform itself to listen to the voiceof users and adapt to their requirements. Conclusion The platform presented in this way, its possibilities, tools, and modules that are in the platform itself, indicate several different conclusions. First, due to a combination of different happy circumstances, we are at a level that is significantly higher than the surrounding countries. Secondly, such a tool provides a significant advantage in the training market, but also the use of such tools by law enforcement agencies. Third, the process of presenting the results and capacity of the platform as a decision aid tool, online investigation tools and multilingual search tools as well as other, no less important, components of the system is restrictive, which significantly limits the possibilities of advertising the platform itself. However, this does not limit such scientific - professional analysis, which can also help in the development and thinking about the wider and further use of the system. It must be acknowledged that such a platform has never existed in our criminal set of tools in the fight against crime. Of course, it can be said that neither the scope nor the forms of crime to which it is directed have ever existed before in this scope. Since it is necessary to fight against such problems with all our might, it is important to include such a tool in the arsenal on the side of the prosecuting authorities. Not only the police and the prosecutor's office will benefit, but also other institutions and calls, such as the Court, but also the bar and citizens in the last resort. Such platforms and tools contribute to strengthening the security of the fight against crime system and, if adequate forms of protection of human rights and freedoms are respected, they have their manifestations in such projects, platforms and weapons behind them, the result cannot be missed. Everyone can benefit from them. Since it is necessary to fight against such problems with all our might, it is important to include such a tool in the arsenal on the side of the prosecuting authorities. Not only the police and the prosecutor's office will benefit, but also other institutions and calls, such as the Court, but also the bar and citizens in the last resort. Such platforms and tools contribute to strengthening the security of the fight against crime system and, if adequate forms of protection of human rights and freedoms are respected, they have their manifestations in such projects, platforms and weapons behind them, the result cannot be missed. Everyone can benefit from them. Since it is necessary to fight against such problems with all our might, it is important to include such a tool in the arsenal on the side of the prosecuting authorities. Not only the police and the prosecutor's office will benefit, but also other institutions and calls, such as the Court, but also the bar and citizens in the last resort. Such platforms and tools contribute to strengthening the security of the fight against crime system and, if adequate forms of protection of human rights and freedoms are respected, they have their manifestations in such projects, platforms and weapons behind them, the result cannot be missed. Everyone can benefit from them. Such platforms and tools contribute to strengthening the security of the fight against crime system and, if adequate forms of protection of human rights and freedoms are respected, they have their manifestations in such projects, platforms and weapons behind them, the result cannot be missed. Everyone can benefit from them. Such platforms and tools contribute to strengthening the security of the fight against crime system and, if adequate forms of protection of human rights and freedoms are respected, they have their manifestations in such projects, platforms and weapons behind them, the result cannot be missed. Everyone can benefit from them.

REFERENCES

Bodrožić, I. (2019). Prikaz projekta NITA iz programa „HORIZONT 2020” *NBP*, Vol. 24, No.1, pp. 95-97, https://doi. org/10.5937/nabepo24-21175.

Headquarters, Department of the US Army (2012). Open-Source Intelligence. Army Techniques Publication No. 2-22.9 (FMI 2-22.9). https://irp.fas.org/doddir/army/atp2-22-9.pdf (31.3.2021).

Ivanović Z. (2016). Dokazne radnje u digitalnom okruženju – kriminalistička analiza, Zbornik radova sa naučno-stručnog skupa sa međunarodnim učešćem *Evropske integracije:pravda, sloboda i bezbednost*, Tara, 24 –26. maj 2016. (367-393). Kriminalističko - policijska akademija i Fondacija „Hans Zajdel”, Beograd.

Ivanović, Z., Lajić, O. & Joka, M. (2016). Korišćenje interneta i rizici po seksualni integritet maloletnika – eksperiment „Krstarica”. *Kriminalistička teorija i praksa*, 3(5), 43–55.

Legal sources

Criminal Procedure Code [Krivični zakonik Republike Srbije] (2011). "Official Gazette of RS No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – CC decision and 62/2021 – CC decision.

Internet

UNODC, in the World Drug Report 2018, underlines that “Fentanyl and its analogues remain a problem in North America, while tramadol - an opioid used to treat moderate and moderate-to-severe pain - has become a growing concern in parts of Africa and Asia. Accessibility of fentanyl and tramadol for medical use is vital for treating pain, but traffickers manufacture them illicitly and promote them in illegal markets causing considerable harm to health”, UNODC, (2018), World Drug Report, www.unodc.org/unodc/en/frontpage/2018/June/world-drug-report2018_opioid-crisis-prescriptiondrug-abuse-expands-cocaine-and-opium-hit-record-highs.html.

https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html (07.2.2021).

https://www.hospitalitynet.org/opinion/4083995.html.

Звонимир ИВАНОВИЋ
Универзитет за криминалистичку истрагу и полицијске студије, Београд

Мина ЗИРОЈЕВИЋ
Институт за упоредно право, Београд

ФУНКЦИОНАЛНОСТ АНИТА ПЛАТФОРМЕ У ПРАВНОМ СИСТЕМУ РЕПУБЛИКЕ СРБИЈЕ

Апстракт

Криминалистичко-полицијски универзитет је ушао у свој први Хоризонт 2020 пројекат 2018. године, са још 16 партнера из укупно 11 земаља у својству организације која обучава припаднике полиције у Републици Србији. Сам пројекат представља јединствен подухват на просторима ЕУ али и шире. Смисао је да истражно оријентисан облик онлајн платформе за претраге дубоког, површинског и тамног интернета у циљу прибављања података о субјектима објектима, везама међу субјектима и доказивања њихових односа и активности. Ова платформа представља јединствено оруђе у борби против нелегалне трговине: наркотицима, новим психоактивним супстанцама, као и фалсификованим лековима, оружјем и муницијом као и финансирања тероризма. Приказ могућности ове платформе укомпонован је са приступом анализи могућих мера и радњи које би дошле у обзир за примену у правном систему Републике Србије. Без обзира на који начин се посматра ова платформа и, иако она представља оруђе примењиво у системима земаља држава чланица ЕУ, неопходно је препознати његову употребљивост и у нашем правном систему Републике Србије. У том циљу пружа се и анализа могућих правних основа за поступање приликом примене оруђа ANITA платформе, као и предлози у вези са могућим процесним радњама које су у опцији за примену. Поред *приказивања специфичности саме платформе и оруђа која са собом носи радом се уједно нуди и елаборација позиционирања овог оруђа у правне оквире наше земље.*

Кључне речи: *ANITA пројекат, процесне мере, посебне доказне радње, OSINT, нелегална трговина.*