Digitization of Migrant Smuggling: Legal and Operational Challenges and Recommendations for Improving the Response in Bosnia and Herzegovina, Serbia, and Montenegro

Belgrade, Sarajevo and Podgorica, July 2025.

Publisher:

Grupa 484
Pukovnika Bacića 3
11040 Belgrade, Serbia

Vaša Prava BiH
Safeta Hadžića 66a
71000 Sarajevo, BiH

Građanska Alijansa
Petra Dedića 26, Građanska kuća
81000 Podgorica, Crna Gora

Authors
Danijela Milešević Plavšić, Goran Delić, Gordana Grujičić, Matea Ćurko, Katarina Najdanović

Editor
Gordana Grujičić

This document was developed with the support of the regional project "SMART Balkans – Civil Society for a Connected Society in the Western Balkans," implemented by the Center for Civil Society Promotion (CPCD), the Center for Research and Policy Making (CRPM), and the Institute for Democracy and Mediation (IDM), and financially supported by the Ministry of Foreign Affairs of the Kingdom of Norway (NMFA). The content of this document is the sole responsibility of the project's authors and does not necessarily reflect the views of the Ministry of Foreign Affairs of the Kingdom of Norway (NMFA) or the SMART Balkans consortium.

Contents

Methodology 5
I Introduction – The Link Between Cybercrime and Migrant Smuggling 7
II State Obligations under the Convention on Cybercrime 9
III Legal Framework for Combating Migrant Smuggling 15
1. Protocol Against the Smuggling of Migrants by Land, Sea and Air 15
2. Alignment of National Legislation with the Protocol 16
2.1. Definition of the Criminal Offense 17
2.2. Sentencing Policy under the Protocol and Convention – Obligations and Standards 22
2.3. Prohibition of Criminal Prosecution of Smuggled Migrants 24
2.4. Information Exchange 25
2.5. Other Preventive Measures – Article 15 25
2.6. Protection and Assistance Measures (Implementation of Article 16 of the Protocol) 26
2.7. Cooperation and Information Exchange (Implementation of Article 17 of the Protocol) 28
III National Mechanisms for Combating Smuggling, Especially in Relation to Digital Technologies 31
IV Challenges in Implementing and Enforcing the Legal Framework for Combating Migrant Smuggling in the Digital Context 33
V Recommendations 35

ABBREVIATIONS

AI	Artificial intelligence
ANPR	Automatic Number Plate Recognition
BIH	Bosna i Hercegovina
CG	Crna Gora
CGNAT	Carrier-Grade Network Address Translation (Mrežna tehnologija za deljenje IP adresa među više korisnika)
VPN	Virtual Private Network (Virtuelna privatna mreža)
EU	Evropska unija
EUROPOL	European Union Agency for Law Enforcement Cooperation (Evropska policijska agencija)
EUROJUST	European Union Agency for Criminal Justice Cooperation (Evropska pravosudna saradnja)
IOM	Međunarodna organizacija za migracije
JIT	Joint investigatioin team
MARRI	Migration, Asylum, Refugees Regional Initiative (Regionalna inicijativa za migracije, azil i izbeglice – Zapadni Balkan)
OCD	Organizacije civilnog društva
OKG	Organizovane kriminalne grupe
OTF	Open Technology Fund (Fondacija koja podržava tehnologije otvorenog koda za digitalna prava i slobode)
OSINT	Open Source Intelligence (obaveštajne informacije iz otvorenih izvora)
RJT	Republičko javno tužilaštvo
RNM	Republika Severna Makedonija
SIENA	Secure Information Exchange Network Application: Bezbedna platforma za razmenu informacija među agencijama za sprovođenje zakona u EU.
SELEC	Southeast European Law Enforcement Center (Centar za sprovođenje zakona jugoistočne Evrope)
UNTOC	United Nations Convention against Transnational Organized Crime (Konvencija Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala)
UNODC	United Nations Office on Drugs and Crime (Kancelarija UN za drogu i kriminal)
UNHCR	United Nations High Commissioner for Refugees (Visoki komesarijat UN za izbeglice)
USDT	Tether (Stabilna kriptovaluta čija je vrednost vezana za američki dolar)
GPS	Global Positioning System (Globalni sistem za pozicioniranje)

Methodology

This document is the result of a regional research study conducted within the framework of a project implemented in Serbia, Bosnia and Herzegovina, and Montenegro from April 2024 to June 2025. The aim of the research was to examine the link between the use of information and communication technologies (ICT) in the context of migrant smuggling and the normative and institutional responses of states that are parties to the Convention on Cybercrime, as well as their obligations arising from the Protocol against the Smuggling of Migrants.

The research was conducted in two phases. ***The first phase*** focused on field data collection, which included semi-structured interviews with migrants and representatives of civil society organizations, as well as data gathered through an online questionnaire. Fieldwork was carried out in various settings, including temporary reception centers, information and support sites for migrants, and online platforms. The research adhered to the principles of confidentiality, voluntariness, and personal data protection, with full respect for ethical standards in research involving vulnerable groups. The questionnaires and interviews were based on the analytical framework defined in the document Methodology for National Inputs on the Modalities of the Use of High Technology ('ICT') by Organized Criminal Groups and the Risks to which Migrants are Exposed, developed in consultation with experts in criminal law, security, cybercrime, and human rights.

The research team documented patterns of digital tool use by smuggling networks, the decision-making processes of migrants, the vulnerabilities they face, and the communication channels between migrants and relevant authorities. During the fieldwork, information was also gathered through meetings with relevant institutions and participation in expert forums. The collected information was consolidated into national reports, which served as the basis for the preparation of this document.

Based on the information collected during the first phase, a methodology was developed for the analysis of the legal framework, with the aim of examining the relationship between the obligations of states party to the Convention on Cybercrime and the legal framework for combating migrant smuggling—the second phase. The ***Second phase*** included a comparative analysis of the legal frameworks in all three countries, focusing on the alignment of national legislation with the provisions of the Protocol and the Convention. Additional interviews were also conducted with investigative bodies, public prosecutors, police structures, and other relevant actors involved in the protection of the rights of smuggled migrants, including independent human rights protection bodies.

The primary objective of this study is to enable a deeper understanding of the growing interconnection between digital crime and migrant smuggling. The study seeks to consolidate and systematize operational data on specific actions taken by smugglers that rely on digital technologies, with particular attention given to whether and to what extent these actions fall under the legal definitions of cybercrime. Based on this analysis, the aim is to identify gaps and inconsistencies in the existing legislation and highlight the need for the introduction of

specific legal qualifications that would facilitate better identification, evidence gathering, and prosecution of digitally facilitated forms of smuggling.

In this regard, we believe that this analytical effort will contribute to a deeper understanding of the complexity of the issue and provide relevant insights that may be useful to policymakers in shaping, developing, and improving strategic and normative responses in this area. Additionally, this type of research and fieldwork provides direct insight into the scope of information held by civil society organizations, which may be relevant for the operational work and investigations conducted by competent state authorities.

An effective and sustainable system for combating migrant smuggling must be based on the consistent application of international standards, particularly those contained in the Protocol against the Smuggling of Migrants by Land, Sea, and Air. In this context, the study provides an overview of the current level of alignment of domestic legislative and institutional frameworks with the provisions of the Protocol, not only in terms of criminalization and the criminal justice response, but also regarding other key obligations assumed by states upon ratifying this instrument.

I Introduction – The Link Between Cybercrime and Migrant Smuggling

Modern forms of migrant smuggling are increasingly taking on the characteristics of high-tech crime. In the digital era, smuggling is no longer limited to the physical transportation of individuals across borders—it has evolved into a complex, transnational operation of high technical and logistical sophistication, where cyberspace plays a central, rather than auxiliary, role. According to reports from Frontex and Europol, smuggling networks operating in the Western Balkans are increasingly relying on digital tools to organize, coordinate, and conceal their activities.[1].

This report analyzes the ways and extent to which digital technologies are used to facilitate irregular migration, based on field research and qualitative data collected in Serbia, Bosnia and Herzegovina, and Montenegro.

Almost all stages of smuggling—from the initial contact with migrants, to logistics, communication, transportation, payment, and verification of "services" rendered—are now conducted, to varying degrees, in digital spaces. The recruitment of migrants (i.e., attracting migrants as clients for smuggling services) typically begins through social media platforms such as Facebook, TikTok, and Instagram, where smugglers post ads "promoting" their services, offering "safe and fast" routes to the European Union. Often, the communication is tailored in the migrants' native languages and supported by visual materials (photos, videos of successful border crossings) with the aim of building trust and demonstrating the smugglers' "professionalism." After the initial contact, communication shifts to closed and encrypted channels on platforms such as WhatsApp, Telegram, and Signal. These platforms are used to exchange key logistical information: coordinates for pick-up and drop-off points, identities of intermediaries, vehicle details, and instructions on how to avoid police checkpoints. According to field reports, it is not uncommon for organizers based abroad (e.g., in Egypt) to monitor the exact location of migrants in transit countries using appropriate navigation apps. Through mobile applications, drivers receive the coordinates of migrant pick-up points only when they are certain that they are not being followed by police. In some cases, official online cameras at border crossings are used to select "less monitored" routes.

The use of pseudonyms, self-deleting messages, and real-time location sharing features allows a high degree of operational flexibility and anonymity. Within the same communication channels, smugglers share photos and videos of migrants as proof that the "service" was successfully completed—these are sent to organizers to authorize payment. These videos

[1] Frontex & Europol (2021), "Digitalisation of migrant smuggling: Digital tools and apps enabling facilitation", Council doc. 12353/21, 29 September 2021, dostupno na: https://www.statewatch.org/media/2870/eu-frontex-europol-digitalisation-migrant-smuggling-report-12353-21.pdf .

often show migrants exiting vehicles, stating their names and country of arrival, or standing in front of recognizable landmarks. In addition to serving as evidence, such content is also used as “marketing material” on social media to attract new clients. Of particular importance is the role of digital space in carrying out financial transactions. Messages and images exchanged within closed groups often include payment codes for the *Hawala* system—a traditional but difficult-to-trace method of money transfer—as well as information about cryptocurrency payments using Bitcoin and Tether. Although the use of digital currencies is not yet dominant, there is a clear perception among smugglers that their use as a payment method is increasing. Their decentralized nature allows transactions to take place outside institutional oversight and without leaving regulatory traces, significantly complicating efforts to track financial flows and identify the actors behind them.

Such a structure of digital communication presents a serious challenge for investigative authorities for several reasons. First, end-to-end encryption prevents the passive interception of communications even when there is a legal basis for it, forcing investigators to rely on physical surveillance of communication (e.g., devices installed in vehicles) or forensic processing of seized devices—methods that are technically demanding, costly, and time-sensitive. Second, self-destructing messages erase evidence before it can be preserved, while virtual numbers and fake accounts further obscure the identities of those involved. Third, even when parts of the communication can be reconstructed, the decentralized and horizontal structure of smuggling networks complicates the identification of roles and hierarchies—there are often no clear links connecting perpetrators with the organizers. In many cases, individuals who physically transport migrants (such as drivers or guides for crossing green borders) have no direct contact with the organizers and receive instructions indirectly, often without knowing the identity of those ordering the operation. Consequently, even when a person is identified, it is legally and technically difficult to prove their integration into a wider criminal structure. In addition, the fast-paced nature of digital communication, the use of multiple devices and accounts, and the fact that many operators act from abroad (often from countries that cooperate in criminal matters), further fragment the flow of information and reduce the effectiveness of traditional investigative methods. In this way, digital infrastructure not only facilitates smuggling but actively destabilizes the legal and technical foundations needed to combat it.

Cases have also been recorded in which technology was abused for extortion purposes. Migrants were kidnapped and abused instead of being transported to their intended destinations, and recordings of the abuse were sent to the migrants’ families via digital apps, accompanied by threats and ransom demands. These methods demonstrate not only the brutality but also the high level of sophistication of the digital criminal environment behind human smuggling. Furthermore, the fact that activities facilitating irregular migration often intersect with cybercrime significantly complicates the situation. For example, there have been cases where smugglers used digital tools to manipulate documents—including the alteration

of e-visas, biometric passports, and residence permits—as well as the creation of fake websites mimicking official migration, visa, or work permit services in order to deceive migrants and profit financially. These criminal practices confirm that migrant smuggling increasingly functions as a complex digital operation, in which traditional migration routes and physical activities are supplemented—and often replaced—by sophisticated cyber components. Although legal frameworks for combating cybercrime exist, the connection between digital crime and migrant smuggling remains underexplored and lacks systematic grounding, preventing an effective institutional response and, in the long term, undermining efforts to combat this form of organized crime. For this reason, the fight against migrant smuggling must include an interdisciplinary and integrated approach that combines criminal investigation, cybersecurity, and forensic expertise, along with international cooperation. It is essential to further investigate the links between cybercrime and smuggling, strengthen digital investigation capacities, and improve the legislative framework to address the complex challenges this form of criminal activity poses to modern states.

II State Obligations under the Convention on Cybercrime

he Council of Europe Convention on Cybercrime, also known as the Budapest Convention[2], is the first and most important international legal instrument focused on combating crime committed through the use of information and communication technologies. Adopted in 2001, the Convention has multiple objectives: to harmonize substantive criminal law in the field of cybercrime among its signatory states, to enable effective and proportionate procedural mechanisms for the collection and preservation of electronic evidence, and to establish a functional framework for swift and reliable international cooperation in combating and prosecuting cybercrime.

The Convention sets forth a comprehensive set of norms and standards that obligate signatory states to establish legislative, institutional, and technical frameworks for identifying, preventing, and prosecuting socially harmful behavior in the digital sphere. In addition to its substantive provisions that define specific cyber offenses, the Convention is notable for its well-developed set of procedural tools that enable competent authorities to apply modern investigative methods, including:

- Expedited preservation of stored data,
- Expedited preservation and partial disclosure of traffic data,
- Production order for data,

[2] The Council of Europe Convention on Cybercrime (Budapest Convention), adopted on November 23, 2001, entered into force on July 1, 2004. The full text of the Convention is available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

- Search and seizure of stored computer data,
- Real-time collection of traffic data,
- Interception of content data.

It is important to emphasize that the Budapest Convention is the only globally accepted and legally binding instrument in this domain that provides concrete, practical tools for state authorities—such as prosecutors, police, and courts—as well as other relevant actors, including specialized technical teams and institutions, to build an effective international mechanism for combating cybercrime.

The Convention criminalizes **nine core forms of cybercrime**:

- **Illegal access** ("hacking"), Article 2;
- **Illegal interception** (eavesdropping on data/communications), Article 3;
- **Data interference**, Article 4;
- **System interference** (e.g., DDoS attacks), Article 5;
- **Misuse of devices** (malware, password crackers, "dual-use" tools), Article 6;
- **Computer-related forgery**, Article 7;
- **Computer-related fraud**, Article 8;
- **Offenses related to child pornography** (possession, distribution, facilitating access), Article 9;
- **Offenses related to copyright and related rights violations** (digital piracy), Article 10.

In addition to the core offenses, the Convention obliges signatory states to criminalize attempts, aiding and abetting, incitement, and transnational forms of the offenses listed above (Article 11). Beyond substantive criminal law, the Convention thoroughly regulates procedural aspects (Section II, Articles 14–21), as well as international cooperation mechanisms (Chapter III, Articles 23–35). Although its procedural provisions are primarily intended for cybercrime, they may also be applied to other criminal offenses when such offenses are committed using digital means or when electronic evidence is necessary for their prosecution. In this way, the Convention attains broader significance beyond the scope of "traditional" cybercrime.

This broader applicability is particularly relevant in analyzing the phenomenon of migrant smuggling. A detailed analysis of the acts involved in the commission of migrant smuggling in practice reveals that many phases of this criminal phenomenon involve elements of cybercrime—ranging from organization and internal communication, the use of encrypted messaging applications, forgery of digital documents, creation of fake websites, and manipulation of digital traces, to the transfer of funds through decentralized systems such as cryptocurrencies. In this context, migrant smuggling may involve specific acts that could be classified (provided other elements of the criminal offense are also met) as offenses under the Budapest Convention, such as: computer-related fraud, forgery, data interference, use of illegal devices, and others.

Therefore, an **integrated approach** is necessary—one that links the fight against cybercrime with anti-smuggling policies—in order to more effectively address the complexity and digitization of contemporary criminal patterns. A comparative overview of these links is presented in the following section:

Description of the action[3]	Link to Migrant Smuggling	Article of the Convention	Serbia (Criminal Code)	Montenegro (Criminal Code)	BiH (Criminal Code)
Illegal access to computer systems or databases without authorization	In the context of migrant smuggling, hackers (or members of organized criminal groups) may access databases containing information on border controls, visa regimes, or police schedules, giving smugglers an advantage. E.g., cases where visa forgers use leaked embassy templates; or access national	Article 2.	Unauthorized access to protected computers, networks, and electronic data processing (Art. 302)	Unauthorized access to computer systems (Art. 353)	Unauthorized access to protected systems and electronic networks (Art. 397)

[3] The actions described in this table represent activities identified during desk research conducted in Serbia, Bosnia and Herzegovina, and Montenegro. They relate to the practices of smuggling networks in the process of facilitating irregular migration that involve or rely on digital technologies.

	registry systems to obtain border and migration control data.				
Use of IP-masking software (VPN, Tor)	Smugglers use VPN services, encryption (e.g., PGP), and anonymity browsers (e.g., Tor) for communication, route planning, and masking IP addresses. These tools are often shared with tutorials in Telegram groups, making it easier for unskilled users to join illegal networks.	Article 6* **Use of VPN/Tor is not a criminal offense per se. However, if distributed or used with the intent to commit crimes under the Convention (e.g., unauthorized system access), Article 6 may apply.*	Making, acquiring, or supplying tools for committing crimes against computer data security (Art. 304a)	Misuse of devices and software (Art. 354)	/
Digital document manipulation – e.g., scanning and altering biometric passports,	Digital forgery using software tools to manipulate .pdf or .jpeg files.	Article 7.	Document forgery (Arts. 355 and 356)	Document forgery (Arts. 412 and 413); making/acquiring/supplying materials for forgery (Art. 262)	Document forgery (Arts. 373 and 374)

e-visas, or residence permits	These forged documents are used to allow migrants access to territories they otherwise could not legally enter.				
Use of self-destructing messaging apps by smuggling networks (used by smugglers or migrants instructed by them)	Use of "wipe tools" and apps with self-destructing messages that auto-delete content or metadata has been observed in migrant smuggling. These actions aim to eliminate digital traces and potential evidence, posing a challenge to investigations.	Article 5.* ** Use of such tools is not a crime per se, but if used to obstruct investigations or destroy evidence, such behavior may fall under Article 5 (system interference), especially where automated deletion of data from digital environments occurs..*	Computer sabotage (Art. 299)* **If aimed at disrupting or impeding electronic data processing relevant to authorities.*	System interference (Art. 350)* **Basic offense applies even if the system/data is not relevant to state authorities; disrupting any system qualifies.*	Computer sabotage (Art. 398)* **If aimed at obstructing electronic data processing relevant to authorities + damage exceeds BAM 500.00 KM*
Online fraud – Using computer	Smugglers set up fake websites offering	Article 8* **This may constitute*	Computer fraud (Art. 301)	Computer fraud (Art. 352)	Computer fraud (Art. 395)

systems to gain unlawful profit	legal migration or asylum services. These sites mimic official agencies to deceive migrants and extract money for non-existent services like visas or residence permits.	*computer-related fraud if a computer system was used to obtain unlawful financial gain.*			
Use of cryptocurrencies and Hawala system	Concealing money flows.	The use of cryptocurrencies and the Hawala system in itself does not constitute a criminal offense under the Budapest Convention, but it may form part of a broader pattern involving criminalized acts, especially when used in combination with tools for concealme	Computer fraud (Art. 301), Money laundering (Art. 245)	Computer fraud (Art. 352), Money laundering (Art. 268), plus special laws on AML/CFT	Art. 395 – Computer fraud, Art. 272 – Money laundering

		nt, data manipulation, or fraud.			

III Legal Framework for Combating Migrant Smuggling

1. Protocol Against the Smuggling of Migrants by Land, Sea and Air

The most important international legal instruments governing the suppression of migrant smuggling, ratified by Serbia, Bosnia and Herzegovina, and Montenegro, are the United Nations Convention against Transnational Organized Crime (UNTOC) and the Protocol Against the Smuggling of Migrants by Land, Sea and Air. While the Convention establishes general measures for combating transnational organized crime, the Protocol specifically regulates this form of crime in the context of migrant smuggling. Together, these instruments enable states to respond comprehensively to the phenomenon of migrant smuggling—particularly important given its cross-border nature and frequent links to other illicit activities such as human trafficking, arms and drug trafficking, or money laundering. The objective of the Protocol is "to prevent and combat the smuggling of migrants, as well as to promote cooperation among States Parties to that end, while protecting the rights of smuggled migrants."

Criminalization

In accordance with **Article 6** of the Protocol, states are obliged to criminalize the following acts when committed for the purpose of obtaining a financial or other material benefit:

- **Migrant smuggling**, defined as *"the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident."* Illegal entry is defined as *"crossing borders without complying with the necessary legal requirements for entry into the receiving State."* (Art. 6, para. 1(a))
- **Enabling unlawful stay**, i.e., allowing a person who is not a national or permanent resident to remain in a state without fulfilling the legal requirements for residence. (Art. 6, para. 1(c))
- **Acts aimed at facilitating migrant smuggling**, including:
    1. Producing fraudulent travel or identity documents (Art. 6, para. 1(b)(i));
    2. Procuring, providing, or possessing such documents (Art. 6, para. 1(b)(ii));

3. Organizing or directing others to commit any of the above offenses (Art. 6, para. 2(c)).

Completion of the offense is not required for criminal liability. According to Article 6, paragraph 2(a), *an attempt to commit any of these offenses* is also considered a criminal offense.

Additionally, the Protocol obliges states to criminalize:

- **Organizing or directing others** to commit the offense of migrant smuggling or related acts (Art. 6, para. 2(c));
- **Attempting** to commit any of the above acts (Art. 6, para. 2(a));
- **Participation**, i.e., the criminal liability of persons involved in the commission of the offense besides the principal perpetrator, in cases of smuggling, enabling unlawful stay, or document forgery (Art. 6, para. 2(b)).

The Protocol also provides that States Parties shall take necessary measures, in accordance with their national legislation, to penalize **transporters** (including companies and owners/operators of transport means) who fail to verify whether passengers possess the required travel documents to enter the receiving state (Art. 11, paras. 3–4).

In addition to the obligation of criminalization, Article 6, paragraph 3 of the Protocol requires states to include **aggravating circumstances** in their legislation, particularly in cases where smuggled persons are subjected to inhuman or degrading treatment, including exploitation, or when the commission of the offense resulted in, or could have resulted in, endangering their life or safety.

The **UNODC Model Law** against the smuggling of migrants proposes a set of optional aggravating circumstances tailored to the specific nature of this offense, which States Parties may incorporate into their legislation. These include: exploiting the vulnerability of migrants for profit; causing injury or death to migrants; prior criminal history; links to organized crime; use of drugs or weapons; smuggling of a large number of persons; official involvement or abuse of public office; involvement of children or pregnant women; exploitation of persons with disabilities; use of or threat of violence; destruction or confiscation of travel documents.

2. Alignment of National Legislation with the Protocol

Serbia, Montenegro, and Bosnia and Herzegovina have incorporated the issue of migrant smuggling into their national legal frameworks by adopting criminal law provisions that define this criminal offense and prescribe appropriate sanctions. However, there are differences in how the acts constituting the criminal offense of migrant smuggling are defined, the conditions related to the offender's financial or material gain, the recognition of aggravated forms of

smuggling, and sentencing policies. These differences reflect the varying approaches of the states in regulating and categorizing smuggling activities, which directly affect legal classification and the severity of penalties imposed in practice.

2.1. Definition of the Criminal Offense

The definition of the criminal offense of migrant smuggling varies across the criminal legislation of the observed countries. In Serbia and Montenegro, it is covered under a single criminal offense, whereas in Bosnia and Herzegovina it consists of several distinct offenses. In the legislation of Bosnia and Herzegovina, the smuggling of migrants is classified as a criminal offense against humanity and values protected under international law, indicating a higher degree of social harm and greater alignment with international standards. In contrast, in Serbia and Montenegro, it is categorized as an offense against public order and peace, which may reflect the legislator's tendency to treat it primarily as a security issue rather than a serious human rights violation.

In all the legal systems analyzed, criminal liability is established for all natural persons—regardless of nationality—who commit the offense within the territory of the state, as well as for acts committed abroad by nationals of that state. In general, criminal liability is also foreseen for legal entities, as well as for natural persons acting on behalf of and for the benefit of legal entities, when the offenses are related to migrant smuggling.

Below is a comparative table presenting how the core obligations under **Article 6 of the Protocol against the Smuggling of Migrants** have been incorporated into the national criminal legislation of Serbia, Bosnia and Herzegovina, and Montenegro, with a focus on the key elements of criminal law incrimination.

Table 1: Criminalization of Acts under Article 6 of the Protocol in National Legislation

Protocol – Article 6 Criminalization	Serbia	BiH	Montenegro
Smuggling of migrants for gain (Art. 6(1)(a))	Article 350(2) CC	Article 189 (1) CC	Article 405(2) CC
Production of false documents (Art. 6(1)(b)(i))	Article 355 (1) CC, Article 356, Article 357	Article 189 (1) CC	Article 412 (1) CC, 413 CC, 414 CC
Acquisition or possession of documents (Art. 6(1)(b)(ii))	Article 355 (1) CC	Article 189 (1) CC	Article 412 (1) CC

Enabling illegal stay (Art. 6(1)(c))	Article 350 (2) CC	Article 189 (2) CC	Article 405 (2) CC
Attempt (Art. 6(2)(a))	Article 30 CC	Article 26 CC	Article 20 CC
Participation (Art. 6(2)(b))	Article 350 (3) CC	Article 189 (3) CC	Article 405 (3) CC
Organizing/Directing others (Art. 6(2)(c))	Article 350 (3) and 350 (4) CC	Article 189a CC	Article 401 CC, 401a CC
Aggravating circumstances (Art. 6(3))	Article 350 (3) CC	Article 189 (3) – (5) CC	Article 405(3) CC

The legislative frameworks of all three analyzed countries largely meet the formal requirements of Article 6 of the Protocol against the Smuggling of Migrants, which concerns the criminalization of the basic forms of smuggling. The core elements of the definition of migrant smuggling—such as facilitating the illegal entry of a person who is neither a national nor a permanent resident of a particular country, with the intent of obtaining material benefit—are incorporated into the criminal laws of all three countries. However, despite the general alignment of the basic definition, there are certain differences in how specific acts constituting the offense are defined and covered by legislation. In some cases, legislators have made the element of material benefit a required component only for certain, but not all, criminalized acts. For example, in Montenegro, the offense of "unauthorized facilitation of the crossing of others across borders" does not require the existence of material benefit as a necessary condition for criminal liability. This opens the door to varying interpretations in practice, depending on the specific conduct of the perpetrator. A similar approach is found in the legislation of Bosnia and Herzegovina, where the definition of the offense includes a wide range of criminalized actions such as recruitment, transportation, concealment, provision of protection, or otherwise enabling the stay of smuggled persons. However, for these acts, the legislator has not established material benefit as a mandatory element of the offense. As in the case of Montenegro, this creates space for interpretations whereby the execution of such acts—though covered by the legal text—could be prosecuted without proving material gain. This may be problematic from the standpoint of full compliance with Article 6 of the Protocol, which emphasizes the element of material or financial benefit as a key distinction between migrant smuggling and other forms of assistance to migrants, including humanitarian aid. On the other hand, the criminal laws of Serbia, Bosnia and Herzegovina, and Montenegro, where they

explicitly require the existence of benefit, state that it may refer to financial or other ("some") benefit, implying that the gain may be either material or non-material. This formulation is formally aligned with the Protocol, which does not require exclusively financial profit, but it still leaves room for varied interpretations in practice—especially in cases where the benefit is not expressed directly in money or tangible goods.

In addition to the aforementioned acts of commission, it is important to highlight that some legislators, within the provisions regulating the criminal offense of smuggling, have also **criminalized activities that do not constitute migrant smuggling within the meaning of the Protocol**. For example, the criminal codes of Montenegro and Serbia broaden the scope of smuggling by including acts such as violent crossings or attempted crossings of state borders, including armed crossings or the use of force. This classification goes beyond the framework established by the Protocol and introduces actions which, under international law, are not considered migrant smuggling. This raises questions about compliance with the precise definitional scope set out in Articles 3 and 6 of the Protocol. Such an approach may lead to legal conflation between smuggling and other offenses related to public order and border security, which would be more appropriately addressed through separate legal provisions rather than those governing migrant smuggling.

Acts **related to the forgery or use of false documentation**—such as the production, procurement, and possession of forged travel documents—are recognized as criminal offenses in all the jurisdictions analyzed. In the legislation of Serbia and Montenegro, these acts are covered under distinct criminal offenses, allowing for their prosecution in concurrence with the offense of migrant smuggling. This approach may result in the imposition of harsher penalties in the event of a conviction, since the same individual may be prosecuted for multiple offenses. In contrast, in the legislation of Bosnia and Herzegovina, acts related to false documentation are included as part of the basic form of the offense of smuggling, which limits the application of the principle of concurrence, but at the same time allows for an integrated approach in qualifying more complex forms of conduct.

All three countries provide for criminal liability for **attempt**, **complicity**, and **organizing or inciting others** to commit the offense. Attempt, complicity, and incitement are regulated through general provisions of criminal law and apply to all offenses, including migrant smuggling. At the same time, acts carried out by a group of individuals—especially by an organized criminal group—are normatively recognized as **aggravating or qualified circumstances**. In Serbia, participation in an organized criminal group is treated as a qualified circumstance within the offense of migrant smuggling itself. In Bosnia and Herzegovina, organizing a group or association for the purpose of committing the offense of "migrant smuggling" is treated as a **separate criminal offense**, regulated by Article 189a of the Criminal Code of BiH. In Montenegro, membership in a criminal group is not addressed within the smuggling offense but is separately criminalized under general offenses of **criminal**

association (Article 401) and **establishing a criminal organization** (Article 401a) of the Criminal Code. This approach in BiH and Montenegro allows for the prosecution of group members independently of the legal qualification of the smuggling act itself, enabling the **cumulative prosecution** of criminal offenses and the imposition of **harsher sanctions in practice**.

With regard to the regulation of aggravating circumstances, all three analyzed countries have incorporated certain qualifying elements into their criminal law provisions on migrant smuggling, in line with Article 6, paragraph 3 of the Protocol. However, despite this formal harmonization, there are substantive differences in how and to what extent these aggravating circumstances are defined in national legislation, which directly affects the legal qualification of the offense, the severity of prescribed penalties, and overall sentencing policy.

In the **Republic of Serbia**, the Criminal Code prescribes aggravating circumstances including the commission of the offense by a group or organized criminal group, abuse of official position, and commission of the offense in a manner that endangers the life or health of smuggled persons, or if a larger number of migrants is smuggled. However, circumstances relating to the **endangerment of migrants' safety**, **their exploitation**, and **inhuman or degrading treatment** are not explicitly recognized as aggravating elements. When these circumstances are present, they may be considered through the **cumulative prosecution of separate offenses**, which in practice complicates consistent and effective prosecution—especially when clear evidence for qualifying the conduct as a separate offense is lacking. A similar approach is observed in the legislation of **Montenegro**. Although basic aggravating circumstances are prescribed, the law does not include provisions addressing the **endangerment of smuggled migrants' safety** or **their exposure to inhuman and degrading treatment or exploitation**. These circumstances, given the specific modus operandi of smuggling networks, are often difficult to qualify as standalone offenses—particularly from the perspective of investigative authorities who face challenges in gathering evidence. Therefore, **explicitly recognizing these circumstances as aggravating factors** within the offense of migrant smuggling would strengthen consistency in criminal justice responses and reinforce the **preventive function** of criminal sanctions. It would allow for the adequate sanctioning of smugglers who transport migrants under conditions that meet the criteria of inhuman treatment or violate the right to safety and human dignity, in line with international human rights standards.

When assessing the degree to which aggravating circumstances have been incorporated into national legislation, it should be noted that even when certain circumstances listed in the Protocol are **not included in the specific article on smuggling**, the general provisions of criminal law still allow judges to **consider relevant facts as aggravating factors** during sentencing. This means a judge can impose a sentence closer to the maximum for the basic form of the offense (e.g., instead of the minimum of 1 year, a sentence closer to the maximum

of 8 years), but this will **not carry the same legal weight** as a sentence for a **qualified form** of the offense (e.g., one with a sentencing range of 5 to 12 years). Thus, while the sentence may be more severe, it would still not reflect the **most serious possible penalty**. In the absence of formal recognition of these circumstances as qualifying elements, there is a greater potential for **legal uncertainty** and **inconsistent judicial practice**, which undermines the uniformity and predictability of sentencing policy.

In contrast to Serbia and Montenegro, the **legislative framework of Bosnia and Herzegovina** demonstrates a **higher level of alignment with international standards**. The Criminal Code of Bosnia and Herzegovina, in addition to prescribing basic aggravating circumstances—such as commission of the offense by an organized group, abuse of official position, and endangering the life or health of smuggled persons—also includes **other key qualifying elements**. These include endangering the safety of smuggled persons, **inhuman or degrading treatment**, commission of the offense against **minors under the age of 18**, and the **death of one or more smuggled persons** as a consequence of the offense. This approach enables more comprehensive recognition of the harmful consequences of smuggling and better protection of victims through the criminal justice system, while respecting the standards set out in international human rights instruments and instruments for combating organized crime. On the other hand, experts in Bosnia and Herzegovina note that the law does not recognize **specific aggravating circumstances stemming from the digital nature** of contemporary smuggling practices, such as the use of **online platforms, cryptocurrencies, encrypted communications, or digital document manipulation**. This opens the door for **further normative improvements** to align the legal framework with the increasingly **technological dimension** of criminal networks.

Example 1: Case Overview – "Zvornik 2023"

In the case prosecuted by the Prosecutor's Office of Bosnia and Herzegovina under the name "Zvornik 2023", the role of digital technologies in the organization of migrant smuggling was clearly evident. The indictment was filed against five individuals who used the Telegram application to recruit migrants from Belgrade and facilitate their transfer across the territory of Republika Srpska toward the EU border. Communication within the group took place exclusively via closed and encrypted Telegram channels, using pseudonyms and automated bots for coordination. Payments were made in the cryptocurrency USDT (Tether), enabling transactions to occur without traces in the traditional banking system. According to the evidence in the indictment, digital wallets located in jurisdictions with a low level of legal assistance were used, further complicating the investigation.

During the investigation, the identities of the migrants and group members were confirmed through analysis of email communications, GPS logs from seized mobile devices, and digital payment reports obtained through international legal assistance. The role of open-source

intelligence (OSINT) was particularly emphasized—investigators identified relevant profiles and connections between participants via social media and dark web forums. In the court proceedings, the Court of Bosnia and Herzegovina concluded that the use of sophisticated digital infrastructure—including encrypted communication channels, anonymous wallets, and online recruitment—constituted an aggravating factor for the conduct of the proceedings and the identification of the perpetrators. However, the judgment did not formally recognize the existence of aggravating circumstances based on the digital elements of the offense. As a result, this case is used as an example of the need for legal clarification of digital forms of smuggling and their qualification.

The "Zvornik 2023" case highlights the growing need to align procedural and substantive law with the realities of modern digital crime, as well as the need to strengthen the capacities of prosecutors, courts, and law enforcement agencies in handling digital evidence, international cooperation, and the legal classification of digitally facilitated forms of organized crime.

2.2. Sentencing Policy under the Protocol and Convention – Obligations and Standards

The **Protocol against the Smuggling of Migrants** does not prescribe specific penalties or sentencing ranges for individual acts, but instead relies on **Article 11(1)** of the **UN Convention against Transnational Organized Crime (UNTOC)**, which requires that sanctions be proportionate to the gravity of the offense. In the case of legal entities, an additional requirement applies under **Article 10(4)** of the Convention, which stipulates that sanctions must be **effective, proportionate, and dissuasive**.

The Protocol does not distinguish, in terms of sentencing policy, between the basic and aggravated forms of the offense—this is left to the discretion of national legislators in the States Parties. Additionally, the Convention obliges States to enable measures for the **confiscation of proceeds** derived from the offense, as well as **property used or intended to be used** in the commission of the offense. In contrast to the Protocol, the **European Union's legal framework**, through the **Council Framework Decision 2002/946/JHA**[4] imposes an obligation on EU Member States to provide for maximum prison sentences of up to eight years in more serious cases—such as when the offense involves financial gain, is committed within a criminal organization, or endangers the lives of smuggled persons. The Directive further requires the possibility of confiscating assets used to commit the offense. Although these obligations do not apply to countries outside the EU, they represent relevant standards for countries in the process of aligning with EU legislation.

[4] Council Framework Decision 2002/946/JHA on strengthening the penal framework to prevent the facilitation of unauthorized entry, transit, and residence.

Table 2: Comparative Table of Sentencing Ranges in Bosnia and Herzegovina, Montenegro, and Serbia

	Form of the Offense	Prescribed Prison Sentence
BiH	Article 189 (1) – Basic form	1-10 years
	Article 189 (2) – Basic form	6 months – 5 years
	Article 189 (3) – Aggravated form	3 – 15 years
	Article 189 (4) – Aggravated form	3 – 15 years
	Article 189 (5) – Aggravated form	At least 5 years
	Article 189 a (1) – Aggravated form	At least 3 years
	Article 189 a (2) – Aggravated form	At least 1 year
Montenegro	Article 405 (2) – Basic form	3 months – 5 years
	Article 405 (3) – Aggravated form	1 – 10 years
Serbia	Article 350 (2) – Basic form	1-8 years
	Article 350 (3) – Aggravated form	2-12 years
	Article 350 (4) – Aggravated form	3-15 years

Compared to the standards established in Council Framework Decision 2002/946/JHA, which requires Member States to prescribe prison sentences of up to eight years for more serious forms of migrant smuggling—namely when the offense is committed for financial gain, by an organized criminal group, or in a manner that endangers the life of the person smuggled—it can be concluded that the legislation of all three countries is formally aligned with these minimum requirements, albeit with certain differences in terms of sentencing ranges, minimum penalties, and differentiation between offense types. For instance, Serbia prescribes a maximum sentence of eight years for the basic form of the offense, thereby meeting the minimum EU standard. Aggravated forms are punished more severely, up to 15 years, in accordance with the seriousness of the circumstances. Bosnia and Herzegovina has the most elaborate system of sentencing provisions, with penalties ranging from six months to 15 years, depending on the form of the offense. The basic form can carry up to 10 years of imprisonment, while the aggravated forms are clearly differentiated, with particularly high minimum sentences when there are elements of violence, death, or child victims. This approach is stricter than the EU standard and reflects a strong penal policy. Montenegro has the lowest sentencing thresholds for the basic form—from three months to five years—while the aggravated form

carries a sentence of up to 10 years, reaching the EU standard only in the most serious cases. Compared to Serbia and BiH, Montenegro's penal framework appears more lenient, especially regarding the basic forms.

2.3. Prohibition of Criminal Prosecution of Smuggled Migrants

Regarding the application of **Article 5 of the Protocol**, which prohibits the criminal prosecution of migrants for having been the object of smuggling, the legal frameworks of the three analyzed countries adopt **different approaches**.

In **Bosnia and Herzegovina**, unlike Article 186 of the Criminal Code, which in paragraph 10 explicitly states that victims of human trafficking shall not be prosecuted for offenses committed as a consequence of being trafficked, no such explicit provision exists for the offense of migrant smuggling under Article 189 or for organizing smuggling under Article 189a. However, based on the definitions and legal constructions (e.g., "who with intent...," "who obtains benefit...," "who organizes..."), it is clear that the migrant, as the object of the offense, cannot fulfill the legal elements of a perpetrator, and thus cannot be held criminally liable under those provisions. In this way, although not explicitly stated, the substantive prohibition under Article 5 of the Protocol is respected.

In **Montenegro**, the legal framework more explicitly recognizes the protection of smuggled migrants, particularly in cases involving victims of human trafficking. Article 54 of the Law on Foreigners provides for a 90-day reflection period for deciding whether to cooperate with the authorities, while Article 55 states that foreigners with humanitarian residence cannot be deported due to illegal entry or stay. In addition, minors who are victims of trafficking are protected from return to countries where they may face danger. Although Article 405 of the Criminal Code prescribes a sentence of up to one year for violent border crossing without authorization, amendments to the Criminal Code from December 2023 (Article 444) clearly state that victims of trafficking who were coerced into participating in criminal activity shall not be punished. This enables the protection of smuggled migrants in cases where there is overlap with trafficking in human beings, significantly aligning the domestic framework with Article 5 of the Protocol.

While the **Criminal Code of the Republic of Serbia** does not contain an explicit provision prohibiting the prosecution of smuggled migrants—unlike the provision for trafficking victims under Article 388, paragraph 6—the lack of criminal liability for smuggled individuals derives from the construction of the offense in Article 350. Since criminal responsibility is attributed exclusively to the person who enables or assists the unlawful entry, stay, or transit of foreigners for gain, the migrant as the object of these acts does not meet the legal criteria of a perpetrator. Thus, despite the absence of an explicit rule, compliance with Article 5 of the Protocol is effectively ensured in **practice**, as smuggled migrants are not held criminally liable.

2.4. Information Exchange

In all three countries, the exchange of information related to migrant smuggling is carried out at the institutional level between competent authorities (police, prosecution offices, immigration services) and in cooperation with international mechanisms (e.g., Interpol, Europol, SELEC). Additionally, information exchange among neighboring Western Balkan countries functions through bilateral and regional police cooperation but remains fragmented and dependent on operational priorities. According to **Article 10** of the **Protocol supplementing the UN Convention against Transnational Organized Crime**, States Parties are required to exchange information concerning: the identity and structure of organized criminal groups, their smuggling methods and means, routes used, misuse of identification and travel documents, as well as new trends and operational patterns. The aim of this obligation is to strengthen an effective and coordinated response to transnational migrant smuggling networks.

In practice, however, significant challenges remain regarding timely, two-way, and systematic information exchange. Improving cross-border data sharing is considered essential for more effective efforts to combat smuggling and the operations of organized criminal groups. This need was recognized at the 4th Annual Regional Meeting of Key Western Balkan Stakeholders in the Fight Against Migrant Smuggling and Human Trafficking[5], where one of the conclusions was that countries in the region should develop interoperable digital platforms to enable faster and more secure data exchange. Such cooperation would support the identification of trafficking and smuggling patterns, enhance regional prevention strategies, and improve responses to cases of labor exploitation.

Although the role of **civil society organizations (CSOs)** in information sharing is not institutionally regulated, CSOs working directly with migrants often have access to crucial field-level data—on routes, incidents, violence, and the actions of smuggling networks. With the establishment of formal cooperation mechanisms and data protection safeguards, CSOs could play a **complementary role** in forwarding information relevant for identifying patterns and preventing smuggling.

2.5. Other Preventive Measures – Article 15

In accordance with **Article 15 of the Protocol**, States Parties are obliged to implement a broad range of preventive measures, including: raising public awareness that smuggling is a criminal activity linked to organized crime and serious risks for migrants; cooperation in public information campaigns to prevent potential migrants from becoming victims; and the

[5] The Annual Regional Meeting of Task Forces from the Western Balkan countries was held from April 7–8, 2025, in Budva, organized by the IOM.

development of social and economic policies addressing the root causes of migration, particularly poverty and underdevelopment.

In practice, however, **Bosnia and Herzegovina**, **Montenegro**, and **Serbia** do not have formal national strategies for implementing these measures in the context of migrant smuggling. In Bosnia and Herzegovina, public information activities targeting migrants are almost exclusively conducted by **civil society organizations** through multilingual brochures, field work, and digital campaigns. In Montenegro and Serbia, institutional measures are **limited and fragmented**, and public awareness campaigns remain **insufficient**. There are no specific preventive actions focused on countering smuggling through **digital technologies**, despite the growing significance of this channel for organized criminal groups.

Civil society organizations already play a key role in **informing and supporting migrants** and could, with institutional recognition and support, actively contribute to the implementation of Article 15—both through direct communication with migrants and through cooperation with local communities and public institutions in raising awareness, gathering data, and creating preventive interventions.

2.6. Protection and Assistance Measures (Implementation of Article 16 of the Protocol)

Given the risk of human rights violations faced by migrants during smuggling operations, it is particularly important to ensure compliance with international human rights law. The Protocol obliges States Parties to take specific measures to identify persons who have been smuggled, provide them with appropriate support and protection, and ensure respect for their internationally recognized rights, especially the right to life and protection from torture or other cruel, inhuman, or degrading treatment or punishment. The right to life includes not only the prohibition of arbitrary deprivation of life but also the state's positive obligation to take appropriate measures to protect individuals whose lives may be at risk. The conditions under which smuggling typically occurs may endanger the physical and psychological health of migrants, and in some cases, the level of risk is such that the absence of emergency medical assistance could amount to a violation of the right to life or the prohibition of torture. Moreover, the fact that a person consented to be smuggled does not necessarily mean they consented to the manner of treatment to which they were subjected during the smuggling process. Smuggled migrants are a highly vulnerable group, often at serious risk of exploitation; it frequently happens that they begin their journey as smuggled migrants but become victims of human trafficking along the way. As irregular migrants, they are subject to criminal prosecution and further vulnerable due to the constant threat of detection by authorities. It is important to note that the personal safety of these individuals is often compromised, as smugglers frequently seize their personal belongings, including money and documents. In accordance with Article 16(3) of the Protocol, a State Party must take into account that persons who have been smuggled may have also been victims of criminal offenses during the smuggling process and must accordingly provide appropriate assistance. As outlined in the Model Law against

the Smuggling of Migrants, depending on the specific case, assistance to smuggled migrants whose life and safety are at risk may include: ensuring physical safety, providing emergency medical and humanitarian assistance and offering legal assistance in procedures aimed at protecting violated or threatened rights.

States are also obligated to take appropriate measures to protect migrants from violence that may be committed against them by individuals or groups due to the fact that they were subjected to smuggling. According to supplementary UNODC guidelines, the standard of "appropriate protection" is interpreted flexibly, in accordance with the specific context of each country. These measures aim to support smuggled individuals once they arrive in the destination country or once they have been identified, in order to prevent their further victimization. The Model Law provides that the content of protective measures should be defined at the national level, taking into account the types of violence smuggled migrants are exposed to, the circumstances under which such violence may occur, the communities and individuals who may be affected, and the means of implementing those measures. In designing and applying the measures, special attention must be given to vulnerable groups, including the specific needs of children and women.

Bosnia and Herzegovina implements protection measures through coordinated cooperation among police agencies, prosecutors, and the Service for Foreigners' Affairs. Migrants identified as smuggled persons are interviewed as witnesses in the presence of court interpreters, after which they are registered and referred to reception centers. In the case of unaccompanied minors, the center for social work is involved to assign a guardian. If indicators of human trafficking are present, the Rulebook on the Protection of Foreign Victims of Trafficking in Human Beings is applied, which provides specific identification and protection procedures. The protection system relies on a functional referral mechanism and institutionally delineated responsibilities, which represents a positive step toward aligning with Protocol standards.

Montenegro has incorporated a multi-layered protection mechanism for smuggled migrants into its domestic legal framework. The Law on Foreigners and the Law on International and Temporary Protection stipulate that migrants who are victims of smuggling are not subject to criminal prosecution but are treated as witnesses or protected persons. A reflection period and the right to reside during proceedings are provided. For minors, there are special procedures in cooperation with social work centers and NGOs. The legal framework is supplemented by strategic documents, including the Strategy on Migration and the Reintegration of Returnees (2021–2025), which indicates a systemic focus on strengthening institutional response.

Serbia implements Article 16 through a combination of legislative provisions, institutional capacities, and strategic plans. The Criminal Procedure Code includes mechanisms for the protection of vulnerable and protected witnesses, including a ban on intimidation, the granting of "particularly vulnerable witness" status, and the application of measures under the Witness

Protection Program. Migrants who cooperate with authorities may be granted temporary residence on humanitarian grounds (Foreigners Act, Articles 61 and 64), although the law lacks detailed provisions on the rights and obligations during such residence, potentially resulting in legal uncertainty. Additionally, the National Judicial Reform Strategy and its accompanying action plans envisage the development of a support services network for witnesses and victims. The role of civil society organizations in providing psychosocial and informational support to smuggling witnesses has also been identified as a potentially valuable resource in empowering migrants' role in criminal proceedings.

In all three analyzed countries, there has been progress in strengthening the normative and institutional mechanisms for the protection of smuggled migrants. However, significant differences remain in the scope and accessibility of protection measures, the level of civil society integration, and compliance with UNODC recommendations. Further progress requires a systemic approach to developing individualized protection measures, the introduction of standardized identification protocols, provision of long-term accommodation and access to basic rights, and full respect for the principles of proportionality, equality, and the best interests of individuals subjected to smuggling.

2.7. Cooperation and Information Exchange (Implementation of Article 17 of the Protocol)

In accordance with Article 17 of the Protocol against the Smuggling of Migrants, States Parties are encouraged to conclude bilateral and regional agreements and arrangements to enhance cooperation in combating this type of crime. According to the interpretation provided in the *Model Law against the Smuggling of Migrants* and the accompanying *Legislative Guide*, the purpose of this article is to establish a legal basis for formalized, institutional, and operational cooperation, including mechanisms such as joint investigation teams, protocols for the exchange of operational data, shared databases, and coordinated operations of police and judicial authorities[6]. The *Model Law* specifically recommends that national legislation authorize competent institutions to conclude such agreements and define within them the practical aspects of cooperation in specific smuggling cases[7].

It is important to note that this obligation is substantively different from the one established under Article 10 of the Protocol, which pertains to the exchange of general information and the provision of training as preventive tools in the fight against smuggling. While Article 10 encourages states to share knowledge on modus operandi, routes, and document forgery techniques, and to develop expert capacities through international trainings and experience exchange[8], Article 17 focuses on legally binding and operationally targeted forms of

[6] Legislative Guide for the Implementation of the Protocol against the Smuggling of Migrants by Land, Sea and Air, UNODC, 2004, paragrafi 92–96.
[7] Model Law against the Smuggling of Migrants, UNODC, 2010, članovi 37 i 38.
[8] Ibid., paragrafi 149–153 (komentari uz članove 29–31 koji se odnose na razmenu informacija i izgradnju kapaciteta).

cooperation. In other words, while Article 10 operates at a strategic and preventive level, Article 17 requires concrete institutional responses and law enforcement mechanisms in real-time, aimed at effectively prosecuting smuggling cases that cross national borders.

Table: Implementation of Article 17 in Serbia, Bosnia and Herzegovina, and Montenegro

Element	Serbia	BiH	Montenegro
Existence of bilateral and regional agreements	Yes – with BiH, Montenegro, North Macedonia; readmission and legal assistance; operational cooperation through Frontex, EUROPOL, SELEC.	Yes – bilateral agreements with Serbia, Montenegro, and Croatia; prosecution protocols on cooperation in combating serious crime; reliance on legal assistance under the European Convention on Mutual Assistance in Criminal Matters.	Yes – bilateral agreements with EUROPOL, Frontex, UNHCR, and IOM; membership in MARRI and SELEC; legal assistance through the European Convention; use of the Convention on Cybercrime in cases involving digital evidence.
Operational real-time information exchange	Established SIENA, INTERPOL, SELEC channels; Ministry of Interior units focused on combating smuggling; participation in OTF operations (including OTF Zebra).	Exists – SIENA and INTERPOL channels; exchange with EUROPOL and through OTF Zebra; operational data exchange via the Service for Foreigners' Affairs and border police units; communication also through SELEC.	Use of SIENA and INTERPOL channels via member institutions; exchange within Frontex joint operations and SELEC; no recorded contribution of CSOs or other actors in information exchange.
Zajednički istražni timovi i operativni centri	Present – JITs through EUROJUST; operational groups comprising MoI–Republic Public Prosecutor's Office–prosecutors; established centers for cooperation in operational investigations.	Ad hoc – participation in JITs and joint investigations with Montenegro and Croatia; operational centers established periodically via OTF Zebra and other working groups with EUROPOL support; focus on swift	Present – participation in JITs supported by EUROJUST; operational cooperation with EUROPOL and use of international legal assistance to gather digital and personal evidence from abroad; focused on

		coordination among prosecutors.	detection and evidence-gathering in cross-border cases.
Institucionalizacija saradnje i mehanizmi praćenja	Present – National contact point for EUROPOL; Anti-Smuggling Department in MoI; permanent working groups with the Republic Public Prosecutor and prosecutors; functional operational centers.	Partial – communication relies on local field offices of the Service for Foreigners' Affairs and border units; lacks a centralized coordination structure, but ad hoc mechanisms function in cooperation with international partners.	Present – institutional cooperation with EUROPOL and EUROJUST; national contact points and coordination within regional projects and forums (MARRI, SELEC); operational integration into international initiatives such as Frontex joint operations.

III National Mechanisms for Combating Smuggling, Especially in Relation to Digital Technologies

Combating migrant smuggling in today's context increasingly requires a transformation of institutional responses, particularly in addressing challenges posed by digitalization. Although all three analyzed countries formally commit to combating smuggling, their responses to the digital dimensions of this phenomenon remain fragmented and insufficiently articulated both normatively and institutionally.

In Bosnia and Herzegovina, despite the existence of certain institutional structures for combatting smuggling—such as the Operational Group composed of representatives of the BiH Prosecutor's Office, SIPA, Border Police, and other competent bodies—there is a lack of an effective and systemic response to the challenges of the digital environment. This group operates without a clearly defined legal status, lacking legislative or sub-legislative regulation, relying solely on informal cooperation. The lack of transparency in its work, absence of publicly available meeting records, and no obligation for regular reporting further hinder institutional oversight and the evaluation of effectiveness in addressing digitally facilitated smuggling. From a technical standpoint, BiH lacks a unified information system that would allow real-time tracking of digital traces, and there is no legal framework obligating internet service providers to preserve and deliver metadata relevant to investigations. Unlike EU member states that apply the Data Retention Directive, BiH has no analogous mechanism, making the collection of digital evidence significantly more difficult. Additional challenges include the lack of standardization in digital records and the absence of interoperability between the information systems of various agencies. Institutions involved in investigations often function in institutional isolation, without information sharing, leading to lost leads, duplicated efforts, and reduced investigation efficiency.

Montenegro also lags in the development of specific operational mechanisms to combat smuggling carried out via digital means. Although the Police Directorate formed mixed operational teams in November 2024 to dismantle migrant smuggling networks—including officers specialized in high-tech crime—the lack of targeted training and specialization in this field limits the scope and effectiveness of their work. The use of digital tools in procedures is largely confined to the forensics phase involving seized devices, with no prior strategic monitoring of digital channels used to organize and direct smuggling operations. A positive step in Montenegro, however, is the plan of the Asylum Directorate of the Ministry of Interior to incorporate questions during asylum interviews regarding the use of digital tools during migration. This initiative, which aims to gather information on apps, forums, social networks, and other digital tools used during the journey, could contribute to identifying smuggling network patterns and enhancing the analytical capacities of competent authorities, while protecting individuals who may be victims.

In the Republic of Serbia, there are certain institutional and technical capacities for combating high-tech crime, particularly through specialized units within the Ministry of Interior and the Prosecutor's Office for Organized Crime. However, despite these capacities, the digital component of migrant smuggling remains underrecognized and unaddressed in the current strategic and legal frameworks. The National Strategy for Combating High-Tech Crime for the period 2019–2023, which has now expired, did not identify migrant smuggling as a distinct form of criminal activity increasingly conducted through digital communication and organizational tools. The strategy focused mainly on areas such as financial cybercrime, online child sexual exploitation, and attacks on information infrastructure, while the smuggling phenomenon remained outside its scope and analytical consideration.

Given that a new national strategy and accompanying action plan for combating high-tech crime are currently being developed, there is an important opportunity to enhance the strategic response. The new strategic documents should recognize the growing interconnection between migrant smuggling and the use of digital technologies, and take into account security findings indicating the increasing overlap between high-tech crime and smuggling activities. This is supported by findings from the Serious and Organized Crime Threat Assessment (SOCTA), which highlight the widespread use of digital tools and technologies in criminal offenses—including tools for anonymous communication (VPN, TOR networks), CGNAT IP address ranges that hinder user identification, and cryptocurrencies used for illicit transactions.[9] Although these findings primarily target high-tech crime, they are highly relevant for understanding the dynamics of contemporary smuggling, which increasingly uses the same mechanisms for organization, payment, and evading detection. Integrating the digital dimensions of migrant smuggling into the new strategic framework would contribute not only to the formal expansion of the definition of high-tech crime but also to strengthening the capacities of competent institutions for developing operational tools and specialized procedures in the field of digital forensics. This would create the foundation for more effective identification and prosecution of networks that use digital channels for migrant recruitment, dissemination of route and border-crossing information, and organizing transport and logistics via messaging apps and encrypted platforms.

In addition, the existing procedures for processing migration cases—both at the operational and administrative levels—currently do not adequately integrate systematic examination of the digital aspects of migration flows. In this regard, there is room to introduce targeted interviews and analytical tools during the processing of asylum applications or other forms of status that would explore the use of digital means during migration. These questions could include, for example, which apps, social networks, forums, or other platforms were used to obtain information about the journey, contact smugglers, find accommodation, or cross

[9] **SOCTA – Threat Assessment Report on Organized Crime in the Republic of Serbia 2023**, Ministry of Interior of the Republic of Serbia – Criminal Police Directorate, Belgrade, 2023, p. 47, p. 123.

borders. Such an approach, while respecting the rights and protection of persons potentially exposed to exploitation, would enable a better understanding of how smuggling networks operate within the digital space.

In this context, the inclusion of civil society organizations (CSOs)—which maintain daily contact with migrants and possess valuable insights into their experiences and patterns of movement and communication—could be important for institutional mechanisms aimed at countering the facilitation of irregular migration. Drawing on the data and information collected by these organizations in the field, in combination with institutional analysis and security assessments, could significantly enhance the overall capacity for early detection of digitally mediated forms of smuggling and for creating effective protection mechanisms. Mechanisms based on cross-sectoral cooperation, horizontal information sharing, and recognition of the contributions of all relevant actors represent a sustainable and strategically grounded path toward strengthening institutional resilience to new forms of crime accompanying the digital transformation of migration movements.

A common denominator across all three countries is the absence of clear strategic positions aimed at integrating digital forensics, inter-institutional cooperation, and normative regulation of the digital environment in the fight against migrant smuggling. In the absence of legal mechanisms mandating the preservation and exchange of digital evidence, without binding inter-agency cooperation protocols, and lacking investment in continuous training and technical infrastructure, the institutional response to the digitalization of smuggling remains reactive, fragmented, and insufficiently effective. This points to an urgent need to improve strategies that address the digital challenges of smuggling through legislative reforms, the development of interoperable systems, and the creation of specialized operational capacities.

IV Challenges in Implementing and Enforcing the Legal Framework for Combating Migrant Smuggling in the Digital Context

Effective implementation of the legal framework for combating migrant smuggling—particularly given the growing use of information and communication technologies by smuggling networks—faces numerous legal, operational, and technical challenges in the countries analyzed. These challenges point to the need for deeper integration of the digital dimension of smuggling into legislative instruments, strengthening the capacity of relevant institutions, improving cross-border cooperation, and developing appropriate technological infrastructure.

In **Bosnia and Herzegovina**, a key challenge is the lack of automated and interoperable information exchange systems between key institutions such as SIPA and the Border Police. There is also no single point of contact for urgent international requests for digital evidence, with cooperation often occurring informally. Moreover, the absence of joint training and

thematic annexes regulating the exchange and processing of digital data significantly limits the effectiveness of cross-border cooperation and real-time responses.

Montenegro faces similar challenges. The current legal framework does not elaborate specific modalities of execution that involve the use of information and communication technologies, and the provisions on covert surveillance are not fully adapted to digital environments. Institutional capacities are limited, coordination between agencies needs improvement, there is a lack of continuous training, and only a small number of specialized teams exist. Technological obstacles include a lack of tools for OSINT analysis, crypto-forensics, predictive analytics, and automated mechanisms for detecting suspicious activity on digital channels. There is no registry of high-risk platforms nor a legal obligation for domestic providers to submit data relevant to investigations.

In **Serbia**, although specialized departments for combating cybercrime and organized crime exist, the digital aspect of migrant smuggling is still not systematically integrated into normative and operational mechanisms. There are no specific legal qualifications that encompass digitally facilitated smuggling, and access to e-evidence remains fragmented and reliant on sectoral initiatives. Operational cooperation between migration, organized crime, and cybercrime departments is not formalized, and data exchange occurs without a unified information system. While technical resources for digital forensics and communication analysis exist, they are underutilized in smuggling cases. There is a lack of systematic preventive campaigns aimed at debunking smuggling messages in the digital space and no monitoring mechanisms for content in the languages of high-risk migration routes.

A common challenge across all three countries is the insufficient linkage between the anti-smuggling and cybercrime sectors. On the other hand, the technological advancement in the use of digital tools by organized criminal groups engaged in migrant smuggling simultaneously represents a significant resource for combating this form of crime. Practice shows that digital tools, when used lawfully and properly, greatly aid in gathering operational and procedural evidence, identifying suspects, and reconstructing criminal networks.

One of the most important instruments in this context includes **special investigative measures**, such as technical surveillance of communications, covert tracking and recording, mobile device location, and the use of advanced digital forensic techniques. The use of drones, ANPR cameras (Automatic Number Plate Recognition), technical devices for tracking vehicles and individuals, and geolocation of mobile phone base stations is becoming standard operational practice in cases of (organized) crime. These methods enable discreet but continuous monitoring and documentation of criminal group activities.

In addition, **specialized cyber units** within police and judicial institutions play a key role in detecting, preserving, and analyzing digital traces—from mobile devices and computers to cloud services and closed digital networks. A defining characteristic of digital evidence is its

distributed nature, rarely stored in one physical location, requiring a holistic approach from the start of an investigation. This type of work bridges the **Protocol against the Smuggling of Migrants** with the **Convention on Cybercrime**, since both instruments—though normatively separate—increasingly require coordinated efforts in practice to identify and prosecute offenders. Likewise, the **active online presence of law enforcement agencies**, including social media monitoring, digital extraction of mobile phone content, and cooperation with internet providers and tech platforms, allows for timely identification of smuggling schemes and high-quality evidence collection. In this way, the internet and digital technologies are not merely spaces of abuse but also powerful tools for **preventing and combating smuggling networks**, thereby affirming their **positive role in protecting migrants and ensuring security**.

V Recommendations

- It is recommended that all aggravating circumstances arising from the Protocol against the Smuggling of Migrants be clearly and explicitly incorporated into the criminal law framework. In particular, migrant smuggling facilitated by digital technologies should be legally recognized as an aggravating circumstance, in order to assist investigative bodies in identifying and qualifying the degree of criminal conduct within the domain of cybercrime—leading to the application of stricter penalties.
- Align national legislation with the Council of Europe Convention on Cybercrime (Budapest Convention) and its additional protocols.
- Fully harmonize the domestic legal framework with EU directives, especially:
- The E-Evidence Regulation;
- The Directive on border protection and oversight of crypto transactions.
- Clarify procedural rules that enable the use of digital traces as valid evidence, along with appropriate safeguards.
- Establish and strengthen a multisectoral operational approach by forming specialized teams for digital investigations and forensics within police and prosecutorial services.
- Ensure continuous training of police officers, prosecutors, and judges in the identification, collection, preservation, and presentation of digital evidence.
- Organize annual simulation exercises ("tabletop exercises") on the theme of smuggling as a digital service.
- Enhance the technical capacities of investigative bodies, particularly in the use of OSINT tools, crypto-transaction analysis, and digital forensics of protected devices.
- Develop new applications with AI components that scan content on social media for human smuggling indicators.
- Strengthen bilateral and multilateral cooperation with international institutions and agencies.

- Consider mechanisms for formalization of the role of civil society organizations (CSOs) in the early warning system, victim identification, and information sharing through legally grounded cooperation protocols, confidentiality mechanisms and data protection.
- Launch digital information campaigns targeting migrants in high-risk languages, as well as campaigns directed at the local population to raise public awareness about the criminal liability associated with migrant smuggling.