

Digital and Technological Solutions in Preventing Human Trafficking and Issues of Rehabilitation

Urinov Odilbek

Operational-Search Department of the Ministry of Internal Affairs of the Republic of Uzbekistan

Received: 22 August 2026 | Received Revised Version: 06 September 2026 | Accepted: 24 September 2026 | Published: 16 October 2026

Volume 08 Issue 10 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue10-05

Abstract

This article provides a criminological analysis of the shift of human trafficking crimes from the traditional physical environment to the virtual space and the sharp increase in their latency. It scientifically substantiates the necessity of implementing modern technological solutions such as digital footprint fixation, Open Source Intelligence (OSINT), Data Mining, Artificial Intelligence (AI), and blockchain forensics to combat this transnational threat. Furthermore, it proposes innovative mechanisms for shifting the focus of victimological prevention from law enforcement agencies to civil society institutions, launching a targeted "Preventive Police" algorithm, and providing social and psychological assistance to victims.

Keywords: Human trafficking, virtual space, digital footprints, artificial intelligence (AI), OSINT, preventive policing, blockchain forensics, digital victimology, social rehabilitation.

© 2026 Urinov Odilbek. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). The authors retain copyright and allow others to share, adapt, or redistribute the work with proper attribution.

Cite This Article: Urinov Odilbek. (2026). Digital and Technological Solutions in Preventing Human Trafficking and Issues of Rehabilitation. The American Journal of Political Science Law and Criminology, 8(10), 26–30. <https://doi.org/10.37547/tajpslc/Volume08Issue10-05>

1. Introduction

Today's globalization and the unprecedented development of information technologies have also caused drastic transformations in the criminal world. As recognized in modern criminology, a severe transnational crime such as human trafficking has now gradually shifted from the traditional environment to the virtual space. Today, transnational criminal groups do not take to the streets to recruit potential victims; they carry out this activity through social networks, fake employment websites, messengers, and even the dark web, without any physical contact. Furthermore, payments are made not in cash, but through cryptocurrencies, which are difficult to trace. This transformation has increased the

level of virtual latency of human trafficking crimes to an unprecedented degree.

Under these conditions, the traditional preventive and operational-search methods (such as neighborhood interviews and visual observation) of the authorities responsible for crime prevention are gradually losing their effectiveness. The shift of the crime of human trafficking from the transnational physical space to the virtual space has set before the science of criminology the task of creating entirely new mechanisms for the early detection of the crime and the mapping of its criminogenic networks. Today, the primary determinants and traces of transnational trafficking are stored not at the crime scene, but in the memories of smartphones, social

network servers, and crypto-wallets.

The views of renowned Russian forensic scientists V.B. Vekhov and E.P. Ishchenko serve as a fundamental basis for creating the scientific and theoretical foundation for combating this new criminal reality. As E.P. Ishchenko points out, modern science is undergoing the largest paradigm shift in its history—now, the main operational field of law enforcement agencies has transformed from the physical space to the realm of “virtual footprints”. Expanding on this theory, V. B. Vekhov emphasizes that digital footprints are significantly more objective than the testimonies of traditional witnesses or victims. From a criminological perspective, the significance of this lies in the fact that a victim may conceal the criminals due to victimological fear, but digital footprints accurately reconstruct the true scale and level of organization of the transnational crime.

However, although mechanisms for extracting these footprints from electronic devices have been developed, their purely criminological significance—that is, their role in creating a complete virtual map of transnational criminal groups—has not yet been fully revealed. As highlighted in the dissertation-level research of A. I. Zazulin, modern digital data is not merely evidence for the court, but rather the single analytical key that exposes the latency of the crime and serves its prevention. .

Collecting the virtual footprints of criminals without losing them is considered the primary task of criminological prevention. The nature of this process is extensively analyzed in the research of S.V.Zuev. As the scientist emphasizes, the application of “Data Mining” methods using specialized software creates the possibility to recover messages, hidden audio and video files, and geolocation history that were deleted by the criminal. The greatest value of the “Data Mining” process for criminological prevention lies in the fact that—through the data extracted from the smartphone of a single apprehended recruiter—we can identify not just a single crime, but the structure of an entire transnational criminal syndicate, the list of other hidden victims, and the next planned trafficking routes.

So, how does this process work in the national practice of Uzbekistan? According to observations, the violation of digital security rules by law enforcement agencies during the inspection of electronic devices is becoming the biggest obstacle to exposing the deep roots of the crime. For example, when a person suspected of human trafficking is apprehended, their smartphone is often left

connected to the network. As a result, the criminal's accomplices are able to remotely delete all correspondence and groups on the network. Consequently, law enforcement agencies apprehend only a single perpetrator, while valuable criminological data regarding the main organizers of the crime and other hidden victims is completely lost.

The urgency of this problem is clearly confirmed by the circumstances of a real criminal case recorded in the Mirabad district of Tashkent city in September 2025. In particular, during a special operation to expose a criminal group that sexually exploited women under the guise of a “Wellness SPA” salon, digital fixation rules were violated when extracting electronic correspondence from the organizer's mobile phone. As a result, not only was the admissibility of this correspondence in court lost, but most tragically – an invaluable criminological-preventive database containing the list of other underage girls planned for recruitment through the criminal's network and the identities of international clients was completely destroyed. This means missing the opportunity to completely dismantle the organized criminal network.

Consequently, there is a need to establish a strict digital methodology in operational-search practices regarding the seizure of electronic devices in human trafficking cases. Specifically, as soon as an electronic device is seized, it must immediately be placed in a “Faraday cage” (a special isolation bag that blocks external signals), and data extraction must be performed using specialized hardware and software complexes. This mechanism not only preserves procedural evidence but also serves to create a complete virtual map of the criminals.

While extracting data from electronic devices is a post-crime process, the ultimate goal of modern criminology is the early prevention of the crime before it even begins. In the fight against human traffickers who operate on a transnational scale and constantly invent new recruitment schemes, traditional methods of statistics and analysis fail to yield the expected results. In this context, the capabilities of Artificial Intelligence (AI) in remotely analyzing massive volumes of data are invaluable.

The scientific conclusions of scholar Q.R. Abdurasulova, who fundamentally researched the problems of crime prevention and criminological forecasting in the context of Uzbekistan, provide the theoretical foundation for this modernization. As the scholar emphasized, for prevention to be targeted and effective, law enforcement

agencies must abandon outdated reporting practices and transition to a system of mathematical modeling of crime dynamics and the application of modern information technologies. That is, the human mind cannot simultaneously combine hundreds of demographic, economic, and criminogenic factors to provide an accurate forecast; an algorithmic approach is necessary for this.

Developing this scientific idea to the level of modern threats creates the necessity to introduce a “Preventive Police” algorithm based on Artificial Intelligence within the system of the Internal Affairs bodies of Uzbekistan and the National Commission. So, how does this innovative model work, and how does it combat human trafficking?

The entire massive database (Big Data) of human trafficking crimes from recent years is loaded into the AI system's “Machine Learning” algorithm. These include thousands of victimogenic indicators, such as the victims' age, place of residence, and marital status; regional unemployment rates, statistics on families with increased credit debt, the number of divorces, and even the dynamics of flight tickets purchased abroad. Artificial intelligence analyzes this massive database in seconds and finds hidden patterns that are invisible to the human eye.

As a result, the AI system predicts with 80-90 percent accuracy, in the form of a probability map, in which district, which neighborhood of the republic, and even among which social stratum (for example, 20-25-year-old divorced women with bank debt) the risk of being drawn into human trafficking will be the highest in the near future. Consequently, prevention inspectors and NGO staff will not waste their resources ineffectively across the entire region, but will instead conduct targeted, focused, and early preventive work exactly in those “red spots” indicated by the Artificial Intelligence and specifically with the at-risk contingent. This makes it possible to eliminate the crime in a purely criminological sense—at the very stage of its preparation.

Considering that today the majority of victim recruitment processes are hidden behind thousands of fake job vacancies, escort services, or advertisements on dating sites, human resources cannot physically read and analyze this constantly updating flow of information. In this regard, as Europol highlighted in its report, the application of Open Source Intelligence (OSINT) and Artificial Intelligence algorithms has become the only

viable alternative solution for law enforcement agencies.

The capabilities of artificial intelligence in the logical and mathematical processing of information have been proven in the models developed by Artur Dubrawski, a professor at Carnegie Mellon University (USA) and one of the leading researchers in this field. In his research, the scientist scientifically substantiates how AI algorithms can detect criminogenic networks among thousands of advertisements. According to him, the AI system scans millions of online advertisements daily using Natural Language Processing (NLP) technology.

For criminology, the greatest significance of this is that AI can logically connect hundreds of advertisements posted in different cities that appear completely unrelated to the human eye. For example, the algorithm analyzes within seconds the hidden forms of telephone numbers in these ads (such as writing the number in words or a mixture of characters), identical specific grammatical errors in the text, or photographs taken in the exact same interior. Through this, it determines that they are all being managed from a single source and provides law enforcement agencies with a clear map of this criminogenic infrastructure.

Today, victim recruitment processes have become completely virtualized. The reality and danger of this problem are clearly confirmed by the recent activities of closed Telegram channels actively promoting intimate services (for example, groups operating under various SPA and massage names). Our analysis shows that such channels constantly change their structure and names, transforming into a massive hidden criminal exchange that connects “clients” and “recruiters” with each other in the virtual space. For each advertisement, criminals accept payments not in cash, but through anonymous electronic wallets or transit bank cards. This massive and constantly shape-shifting virtual flow cannot be physically analyzed using traditional methods. In this context, the application of Open Source Intelligence (OSINT) and Artificial Intelligence algorithms is the single irreplaceable solution for prevention and early detection.

So, which specific AI programs might be beneficial for our national criminological practice in this regard? First and foremost, we can point to the “Memex” project created by the US Defense Advanced Research Projects Agency (DARPA). As is known, standard search engines index only 5-10 percent of the internet. The remaining 90 percent (the Deep Web) is closed to traditional preventive

surveillance. The “Memex” program created by DARPA is a specialized Artificial Intelligence weapon that specifically scans this closed “dark web” and proactively identifies virtual recruitment channels belonging to human traffickers.

Today, the “Traffic Jam” artificial intelligence tool, developed by Marinus Analytics based on “Memex”, has become a daily criminological and preventive tool for US and European police. This program conducts deep analysis not only of text but also of photographic materials. If a criminal transport a victim to another country and posts a new advertisement, the “Traffic Jam” system recognizes the victim from details in the background of the photograph and automatically maps the trafficking route of the transnational criminal group.

Another important direction of modern technologies in preventing human trafficking is victimological identification, that is, rescuing victims through the early identification of their identities. Practice shows that during the process of selling victims (especially minors) over the internet, transnational criminals hide their facial features in photographs using graphic filters. Under such conditions, it is impossible to recognize the victim with the human eye and provide them with victimological assistance. In solving this problem, the experience of the “Spotlight” artificial intelligence program, developed by the US non-governmental organization “Thorn”, is unparalleled.

The program continuously scans the internet and automatically compares these images with the biometric geometry of missing persons on search lists. Рус криминалист олими К.А. Сергеев таъкидлаганидек, алгоритм суратдаги шахсининг кўз қорачиқлари орасидаги масофани, юз суягининг тузилишини миллиметрик аниқликда ўлчайди. This technology makes it possible to rapidly identify our missing citizens among thousands of unknown individuals abroad and place them under timely victimological protection (rescue them).

The most crucial and final stage of the criminological fight against transnational human trafficking is severing the economic determinants (financial roots) of the crime. Global experience demonstrates that today, major criminals utilize anonymous crypto-wallets and digital assets (Bitcoin, USDT) to launder their proceeds. As a conceptual solution to this, the method of “Blockchain Forensics” is recognized in the reports of the UN (UNODC).

Using this method, a qualified analyst, utilizing specialized software (Chainalysis, Crystal Blockchain), traces the virtual movement graph of funds originating from the criminal's crypto-wallet and automatically detects them at the moment they are cashed out on official international crypto-exchanges. Since the exchanges are required to identify their clients according to FATF rules, the true identity of the criminal is exposed. This, in turn, allows the law enforcement agencies of Uzbekistan to completely paralyze the virtual financial channels of organized criminal groups (leaving them without economic resources).

In combating the virtualization of human trafficking, it is necessary to establish the institution of “digital victimology.” Here, OSINT and artificial intelligence technologies are applied not for operational-search purposes, but for the early detection of criminogenic risks and social prevention. The “Digital Victimological Monitoring” system, to be established under the National Commission and NGOs, will analyze suspicious advertisements on the internet and ensure the automatic delivery of warning and legally-oriented preventive content to the devices of potential victims. According to the analyses studied during the research, although a number of systemic reforms have been implemented in recent years in the field of combating human trafficking, the current mechanisms for identifying victims, providing them with social, legal, and medical assistance, rehabilitating them, and reintegrating them into society do not fully meet today's pressing requirements. It was found that the practice of early detection and identification of victims is not sufficiently regulated, and rehabilitation services are not fully established.

In our opinion, in order to further improve the system for combating human trafficking, to expand the opportunities for individuals who are victims or presumed victims of human trafficking (hereinafter referred to as victims of human trafficking) and their families to use social services and receive assistance, to early identify the needs of individuals in risk groups, as well as to align national legislation with international standards and ensure the guaranteed protection of human dignity and labor rights, it is necessary to adopt a Decree of the President of the Republic of Uzbekistan “On Improving the Activities to Combat Human Trafficking and Developing the Rehabilitation System” (Appendix 11).

In the era of globalization and digitalization, the forms of

human trafficking are evolving and migrating into the virtual space (social networks, hidden messengers). This Decree establishes the legal foundation for an in-depth scientific analysis of these new manifestations of crime, the early identification of “risk groups” and the adaptation of preventive mechanisms to modern threats.

As a result of researching the conceptual foundations of combating human trafficking, improving inter-agency cooperation, and applying the capabilities of digital technologies and artificial intelligence to victimological forecasting, the following generalized scientific and practical conclusions and proposals are put forward:

Firstly: Considering that law enforcement agencies primarily focus on investigating committed crimes and punishing perpetrators, whereas civil society institutions (non-governmental organizations, psychological support centers, the mahalla, and family support structures) can directly and positively influence the deep roots of the problem—such as family conflicts, psychological trauma, social isolation, and economic dependence—it is recommended to shift the center of gravity of victimological prevention from law enforcement agencies to the civil society sector.

Secondly: In order to localize the root causes of human trafficking, it is necessary to abandon “universal templates” in prevention and transition to targeted forecasting based on the unique “Regional Crime Map” of each region. In this process, a “National Database for Victimological Forecasting” based on “Big Data” and Artificial Intelligence technologies should be created, and a “Preventive Police” algorithm that predicts risks in advance should be launched for prevention inspectors.

Thirdly: To identify and eliminate the risks of human trafficking, it is deemed necessary to introduce a “National Registry of Human Trafficking Risks” which will record dangerous situations and criminogenic channels that lead to human trafficking. Furthermore, this registry should specifically flag unverified foreign job vacancies, unlicensed intermediaries, suspicious job offers on social networks, and disguised proposals such as “massage”, “SPA”, “high income” or “we will cover travel expenses” along with unknown recipients abroad, repetitive flight routes, medical and social environments with a risk of infant trafficking, and conditions involving the confiscation of passports or the subsequent working-off of travel expenses.

References

1. Вехов В.Б., Ищенко Е.П. Криминалистическое изучение электронной жизнедеятельности человека: монография. / Virtual Forensics. – Moscow: Prospect, 2018. – P. 34-40.
2. The same source.
3. азулин А.И. Использование цифровой информации в доказательстве по уголовным делам. Diss. ... Candidate of Legal Sciences. - Тошкент, 2018. – P. 58-64.
4. Zuev S.V. Fundamentals of Electronic Evidence Theory. Monograph. – M.: Yurlitinform, 2019. – P. 112-118.
5. From the materials of the investigative practice of the Investigative Department of the Tashkent City Main Department of Internal Affairs for 2025-2026.
6. Abdurasulova K.R. Criminological problems of crime forecasting and ways to solve them. // Rights and Duties. - 2021. - 5. No – P. 34-38.
7. Europol. Trafficking in Human Beings in the Digital Age. – The Hague: Europol Public Information, 2020. – P. 14-18.
8. Dubrawski A., Miller K., Barnes M., et al. Data Mining and AI for Combating Human Trafficking. // IEEE Xplore: Global Humanitarian Technology Conference (GHTC). – 2015. – P. 34-40.
9. DARPA (Defense Advanced Research Projects Agency). Memex Program Overview. // Official Report. – Washington, D.C., 2015. (In the text, this is where DARPA and Memex are mentioned.)
10. Marinus Analytics. “Traffic Jam” Suite: Empowering Law Enforcement. – Pittsburgh, 2021.
11. Thorn. Spotlight: Empowering Law Enforcement to Identify Victims of Child Sexual Abuse and Human Trafficking. – Annual Report. San Francisco, 2021. – P. 12-16.
12. Сергеев К.А. Использование цифровых следов и алгоритмов искусственного интеллекта при расследовании киберпреступлений и торговли людьми. Diss. ... Candidate of Legal Sciences. – М., 2022. – P. 134-139.
13. UNODC & ITU. Cybercrime and Technology-Facilitated Trafficking in Persons. Joint Global Report. – Vienna/Geneva, 2021. – P. 85-92.