

Procedural Transformation of Digital Evidence in Human Trafficking Cases: A Doctrinal Analysis of Kazakhstan's Evidentiary Framework

Assem Alimkhanova^{1*}

¹ Department of General Legal Disciplines, Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Republic of Kazakhstan

*Corresponding Author Email: assemalimkhanova22@gmail.com

ABSTRACT

Human trafficking increasingly generates operational, documentary, and digital information, yet the availability of such information does not necessarily determine whether it can function as evidence in criminal proceedings. This study aims to examine the evidentiary structure of human trafficking proceedings in Kazakhstan by identifying the circumstances that must be proved, analysing how operational-investigative information acquires evidentiary value, and assessing the legal treatment of digital evidence. The study employs a normative/doctrinal legal research design based on primary legal materials, including Kazakhstan's Penal Code, Criminal Procedure Code, Law on Operational Investigations, Law on Countering Human Trafficking, Digital Code, and relevant Supreme Court normative interpretations. The materials were analysed through three sequential stages: normative identification of circumstances subject to proof, procedural analysis of the transformation of investigative information into evidence, and a *lex lata-gap-risk-lex ferenda* analysis of digital evidence. The findings show that, first, the structure of proof in trafficking cases is offence-specific and multi-layered. Second, operational-investigative information and evidence capable of judicial use are not legally equivalent; evidentiary value depends on lawful procedural transformation, verification, fixation, and evaluation. Third, Kazakhstan already recognises various forms of digital information, but the applicable rules remain fragmented with respect to authentication, attribution, integrity, preservation, the digital chain of custody, and cross-border electronic evidence. The study implies the need for more coherent procedural guidance and digital forensic safeguards without weakening existing admissibility standards. Its originality lies in developing the concept of procedural transformation and integrating substantive proof requirements, investigative information, and digital-forensic safeguards into a hybrid evidentiary model for human trafficking proceedings.

Keywords: Admissibility; digital evidence; human trafficking; Kazakhstan; procedural transformation.

ABSTRAK

Perdagangan manusia semakin menghasilkan berbagai bentuk informasi operasional, dokumenter, dan digital, tetapi ketersediaan informasi tersebut tidak dengan sendirinya menentukan apakah informasi itu dapat berfungsi sebagai alat bukti dalam proses pidana. Penelitian ini bertujuan untuk menganalisis struktur pembuktian dalam perkara perdagangan manusia di Kazakhstan dengan mengidentifikasi keadaan yang harus dibuktikan, menganalisis bagaimana informasi hasil kegiatan operasional-investigatif memperoleh nilai pembuktian, serta menilai pengaturan hukum terhadap bukti digital. Penelitian ini menggunakan desain penelitian hukum normatif/doktrinal yang berbasis pada bahan hukum primer, meliputi Kitab Undang-Undang Hukum Pidana Kazakhstan, Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang tentang Kegiatan Operasional-Investigatif, Undang-Undang tentang Penanggulangan Perdagangan Manusia, Digital Code, serta interpretasi normatif Mahkamah Agung yang relevan. Bahan hukum dianalisis melalui tiga tahap berurutan, yaitu identifikasi normatif terhadap keadaan yang harus dibuktikan, analisis prosedural mengenai transformasi informasi investigatif menjadi alat bukti, dan analisis *lex lata-gap-risk-lex ferenda* terhadap bukti digital. Hasil penelitian menunjukkan bahwa, pertama, struktur pembuktian dalam perkara perdagangan manusia bersifat spesifik terhadap bentuk tindak pidana dan berlapis. Kedua, informasi operasional-investigatif dan bukti yang dapat digunakan dalam proses peradilan tidak

* Copyright (c) 2026 **Assem Alimkhanova**

This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

Received: December 8, 2025; Revised: July 7, 2026; Accepted: August 14, 2026

memiliki kedudukan hukum yang sama; nilai pembuktian bergantung pada transformasi prosedural yang sah, verifikasi, pencatatan, dan evaluasi. Ketiga, Kazakhstan telah mengakui berbagai bentuk informasi digital, tetapi ketentuan yang berlaku masih terfragmentasi dalam aspek autentikasi, atribusi, integritas, preservasi, rantai penguasaan bukti digital, serta bukti elektronik lintas batas. Penelitian ini mengimplikasikan perlunya pedoman prosedural yang lebih koheren serta mekanisme pengamanan forensik digital tanpa mengurangi standar penerimaan bukti yang telah berlaku. Orisinalitas penelitian terletak pada pengembangan konsep transformasi prosedural dan integrasi persyaratan pembuktian substantif, informasi investigatif, serta pengamanan forensik digital ke dalam model pembuktian hibrida untuk perkara perdagangan manusia.

Kata kunci: Penerimaan bukti; bukti digital; perdagangan manusia; Kazakhstan; transformasi prosedural.

INTRODUCTION

Human trafficking presents distinctive difficulties for criminal investigation and proof because the offence may involve multiple participants, stages of conduct, jurisdictions, and forms of exploitation. These difficulties have become more pronounced as trafficking activities increasingly intersect with digital technologies. Internet technologies can facilitate recruitment, communication, control, advertising, financial transactions, and exploitation, while simultaneously generating digital traces that may become relevant to criminal investigations. The United Nations Office on Drugs and Crime (UNODC, 2020), in an analysis of 79 trafficking cases involving internet technologies across more than 30 jurisdictions, documented the use of social media, webpages, communication applications, and other digital platforms in recruitment and exploitation. The same technological environment may therefore serve both as an instrument for facilitating trafficking and as a source of evidentiary information for law-enforcement authorities. However, the existence of digital information does not automatically resolve the legal question of whether such information can be reliably authenticated, preserved, attributed, and admitted as evidence.

The legal significance of this issue is particularly evident in Kazakhstan, where the regulatory framework governing human trafficking and digital information has recently undergone substantial development. Human trafficking is criminalised principally under Article 128 of the Penal Code, while Article 135 separately regulates trafficking in minors (Penal Code of the Republic of Kazakhstan, 2014, Arts. 128, 135). The Criminal Procedure Code establishes the general framework for evidence, circumstances subject to proof, investigative actions, covert investigative actions, admissibility, reliability, and evidentiary evaluation (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111–125, 231–245). In 2024, Kazakhstan adopted a dedicated Law on Countering Human Trafficking, which established the organisational and legal basis for a unified system of prevention, investigation, victim identification, protection, and international cooperation (Law on Countering Human Trafficking, 2024). This framework was followed by the Digital Code of 2026, which introduced updated regulation of electronic documents, digital documents, digital data, and electronic digital signatures (Digital Code of the Republic of Kazakhstan, 2026, Arts. 49–50, 62–64). These developments create a timely need to examine how different legal regimes interact when trafficking is established through both conventional and digital sources of information.

Previous scholarship relevant to this problem can be organised into three principal streams. The first addresses human trafficking as an organised and difficult-to-investigate criminal phenomenon. Pajón and Walsh (2020) develop a theoretical framework for trafficking investigations and emphasise the complexity of reconstructing trafficking conduct through criminal-investigative processes. Bjelland (2020) demonstrates that success in trafficking policing cannot be evaluated solely through conventional

enforcement outcomes, because investigative effectiveness is influenced by institutional, evidentiary, and victim-related considerations. Nastas (2024) similarly examines the specific characteristics of human trafficking investigations and the investigative measures required to identify and reconstruct trafficking schemes. This literature demonstrates that trafficking demands a coordinated and multi-source investigative response, but it focuses primarily on the organisation and effectiveness of investigation rather than on the precise legal transition from investigative information to judicial evidence.

A second body of scholarship focuses more directly on the evidentiary and prosecutorial dimensions of trafficking. Ward and Fouladvand (2021) demonstrate the significance of expert evidence while also emphasising the need to scrutinise the reliability and limits of expertise in trafficking proceedings. Hounmenou and Toepp (2023) identify collaboration, victim-centred practice, and information gathering as important elements of trafficking investigations, while Nichols and Heil (2024) propose an integrated prosecution model that incorporates survivor-centred and restorative approaches. These studies show that trafficking prosecutions depend on multiple actors and evidentiary sources and that victim testimony cannot be considered in isolation from other forms of corroboration. Nevertheless, this literature does not fully explain the doctrinal mechanisms through which operational information, investigative outputs, documents, expert findings, and other factual materials acquire the procedural status necessary for judicial use.

A third stream examines the growing relationship between trafficking and digital technology. De Vries and Radford (2022) demonstrate that online environments contain identifiable risk markers that can support the detection of trafficking and other hard-to-observe crimes. UNODC (2020) similarly documents the use of digital platforms in recruitment, advertising, communication, and exploitation. At the international policy level, the Working Group on Trafficking in Persons has emphasised that technology-facilitated trafficking requires domestic legal frameworks that support lawful digital investigations and the effective use of electronic evidence (United Nations Office on Drugs and Crime, 2021). The same UNODC analysis notes that digital evidence may document working conditions, threats, transport logistics, financial activity, and forms of control, while cross-border electronic evidence requires expertise in acquisition, preservation, sharing, and digital forensics (United Nations Office on Drugs and Crime, 2021). Thus, existing research establishes the growing investigative value of digital information, but the literature has focused more strongly on detection, technological opportunities, and investigative practice than on the internal structure of evidentiary admissibility.

These three research streams remain insufficiently integrated. The existing literature does not fully connect the substantive circumstances that must be proved legally, the procedural mechanisms by which investigative information becomes evidence, and the specific evidentiary problems created when the underlying information is digital. This gap is particularly important in Kazakhstan. The relevant rules are distributed across the Penal Code, the Criminal Procedure Code, the Law on Operational Investigations, the Law on Countering Human Trafficking, the Digital Code, Supreme Court interpretations, and international legal instruments. Consequently, the central problem is not simply whether investigators possess modern digital tools or whether digital information can be collected. The more fundamental question is how heterogeneous information is legally transformed into evidence whose relevance, admissibility, reliability, authenticity, integrity, and provenance can withstand judicial scrutiny.

This study addresses that gap by shifting the analytical focus from the description of investigative techniques to the evidentiary architecture of human trafficking proceedings. Its contribution lies in examining three successive legal questions. First, it identifies the circumstances and constituent elements that must be proved under Kazakhstan law and demonstrates that proof of trafficking is offence-specific

rather than governed by a single, undifferentiated formula. Second, it examines the legal transition from operational-investigative information to evidence capable of judicial use, conceptualising this transition as a process of procedural transformation. Third, it evaluates the existing legal treatment of digital information and distinguishes the rules that currently constitute *lex lata* from additional forensic and procedural safeguards that may be considered *lex ferenda*. The originality of the study, therefore, lies not in introducing screenshots, metadata preservation, or other digital techniques as technological innovations, but in locating these forms of information within a coherent procedural model of criminal proof.

Accordingly, the objective of this study is to analyse the normative and procedural structure through which evidence is established and used in human trafficking proceedings in Kazakhstan, with particular attention to digital evidence. The study addresses the following research questions: What circumstances and constituent elements must be proved in human trafficking proceedings under Kazakhstan law? Through what procedural mechanisms does operational-investigative information acquire evidentiary value in criminal proceedings? How does Kazakhstan's current legal framework regulate digital evidence in human trafficking cases, what procedural gaps remain, and what additional safeguards are required?

These research questions correspond to three interconnected levels of analysis: the normative structure of proof, the procedural transformation of investigative information, and the legal treatment of digital evidence. This structure also avoids treating investigative information and judicial evidence as legally equivalent. Under Kazakhstan's criminal-procedural framework, factual usefulness alone is insufficient; information must enter proceedings through recognised evidentiary mechanisms and remain subject to the requirements of admissibility, reliability, verification, and sufficiency (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111–125).

This article argues that the central weakness of the current evidentiary framework is not the absence of legal recognition of digital information, but the fragmentation of the procedural rules by which different forms of information are transformed into reliable evidence for judicial use. Kazakhstan law already recognises computer information and technically recorded materials within existing evidentiary categories, while the Digital Code regulates several forms of legally significant digital information (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 118–120; Digital Code of the Republic of Kazakhstan, 2026, Arts. 49–50, 62–64). However, the interaction among substantive criminal law, operational-investigative activity, criminal procedure, digital regulation, and cross-border cooperation does not yet provide a uniform procedural framework for authenticity, integrity, provenance, attribution, preservation, and reproducibility across heterogeneous digital evidence. The study therefore proposes a hybrid evidentiary model in which offence-specific circumstances determine what must be proved; operational and investigative information is incorporated through legally recognised procedural mechanisms; digital-forensic safeguards support authenticity and integrity where the source is digital; and all resulting evidence remains subject to the general judicial standards of relevance, admissibility, reliability, and sufficiency.

METHODS

This study employed a normative/doctrinal legal research design to examine the evidentiary structure of human trafficking proceedings in Kazakhstan, with particular attention to the procedural treatment of operational-investigative information and digital evidence. The unit of analysis was therefore not individual trafficking cases, interviews, or survey responses, but authoritative legal texts and legally

relevant documentary materials. Primary legal materials constituted the principal data for the study, while academic literature and technical guidance served as secondary sources for interpretation, comparison, and the formulation of recommendations. The legal corpus was selected for its direct relevance to the three research questions: the circumstances that must be proved, the procedural mechanisms by which investigative information acquires evidentiary value, and the regulation and admissibility of digital evidence.

The primary legal materials consisted of the Penal Code of the Republic of Kazakhstan, particularly Articles 128 and 135 governing trafficking in persons and trafficking in minors; the Criminal Procedure Code of the Republic of Kazakhstan, particularly Articles 111–125 governing evidence and proof and Articles 231–245 governing covert investigative actions; the Law on Operational Investigations, particularly Articles 2, 10–11, 14, and 14-1; the Law on Countering Human Trafficking No. 110-VIII of 5 July 2024; and the Digital Code of the Republic of Kazakhstan No. 255-VIII of 9 January 2026 (Criminal Procedure Code of the Republic of Kazakhstan, 2014; Digital Code of the Republic of Kazakhstan, 2026; Law on Countering Human Trafficking, 2024; Law on Operational Investigations, 1994; Penal Code of the Republic of Kazakhstan, 2014). Judicial interpretation was examined through the Normative Decree No. 7 of the Supreme Court of the Republic of Kazakhstan of 29 December 2012 on the enforcement of legislation establishing liability for human trafficking, as amended through 2024, and the Regulatory Resolution No. 5 of 11 December 2020 on the authorisation of covert investigative actions (Supreme Court of the Republic of Kazakhstan, 2012, 2020). These materials were examined in their consolidated versions available through Kazakhstan's official Adilet Legal Information System as of August 2026.

International law was used selectively rather than as a separate, broad comparative corpus. The principal international instrument was the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organised Crime, particularly Article 3, which concerns the definition and constituent elements of trafficking (Protocol to Prevent, Suppress and Punish Trafficking in Persons, 2000). International materials were used to contextualise Kazakhstan's substantive trafficking framework and to assess points of correspondence with international standards. The study did not undertake a country-by-country comparative analysis. Accordingly, international human rights instruments that did not directly address the research questions were not treated as principal analytical materials.

The doctrinal analysis was conducted in three sequential stages corresponding directly to the three research questions and Results sections. In the first stage, substantive criminal-law provisions were read together with Article 113 of the Criminal Procedure Code and the Supreme Court's authoritative interpretation to identify the circumstances and constituent elements that must be proved in trafficking proceedings. Particular attention was given to the distinction among purchase or sale, other transactions concerning a person, recruitment, transportation, transfer, harbouring, receipt, exploitation, and other acts directed toward exploitation, as well as to the differing requirements concerning direct intent, exploitative purpose, victim-related circumstances, aggravated forms of the offence, participation of multiple offenders, and resulting harm (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 113; Penal Code of the Republic of Kazakhstan, 2014, Arts. 128, 135; Supreme Court of the Republic of Kazakhstan, 2012). The results of this stage were synthesised into the Normative Matrix of Circumstances to Be Proved, presented in Table 1.

The second stage examined the procedural transformation of investigative information into evidence capable of judicial use. The analysis traced the legal status of information from operational-investigative activity through recognised criminal-procedural mechanisms and ultimately to evidentiary

evaluation. Article 14 of the Law on Operational Investigations was analysed together with Articles 111–125 of the Criminal Procedure Code to determine when operational materials may be used in proving and how factual data are collected, fixed, examined, and evaluated (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111–125; Law on Operational Investigations, 1994, Art. 14). Covert investigative actions were analysed separately under Articles 231–245 of the Criminal Procedure Code and the Supreme Court's Regulatory Resolution No. 5 of 2020 because Kazakhstan law expressly distinguishes covert investigative actions conducted within criminal proceedings from operational-search measures conducted under operational-investigative legislation (Supreme Court of the Republic of Kazakhstan, 2020). This stage produced the Procedural Transformation Matrix presented in Table 2 and enabled the study to distinguish among operational information, criminal-procedural investigative actions, and evidence suitable for judicial use.

The third stage applied a *lex lata*–gap–risk–*lex ferenda* analytical framework to digital evidence. First, the study identified what Kazakhstan's current law expressly regulates concerning computer information, electronic documents, digital documents, digital data, recordings, digital devices, covert acquisition from computers and servers, and cross-border legal assistance (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 118–125, 197, 199, 231–245; Digital Code of the Republic of Kazakhstan, 2026, Arts. 49–50, 62–64; Law on Countering Human Trafficking, 2024, Art. 12). Second, the legal texts were examined for areas in which regulation remained absent, fragmented, unclear, or insufficiently specific in relation to screenshots, screen recordings, metadata, social-media and messenger data, archived webpages, digital copies, device-derived information, integrity verification, digital chain of custody, and foreign-held platform data. Third, the evidentiary risks associated with these gaps were identified across authenticity, attribution, provenance, integrity, preservation, and admissibility. Finally, technical practices such as forensic copying, cryptographic hash verification, metadata preservation, source documentation, and a documented chain of custody were considered only as recommended procedural safeguards (*lex ferenda*), rather than as requirements of current Kazakhstan law. Authoritative digital-evidence guidance was used for this limited normative function (Guttman et al., 2022; Kent et al., 2006). The findings were synthesised in Table 3.

The study applied a hierarchical and cross-referential method of legal interpretation. Primary legislation and Supreme Court normative interpretations were given priority over secondary academic commentary. Individual legal propositions were checked against the specific provision that directly governs the issue, rather than being inferred from general treaties or secondary literature. Statutory provisions were interpreted systematically by examining their relationship with other relevant provisions, while the Supreme Court's normative resolutions were used to clarify the operation of substantive and procedural rules. Secondary literature was used principally to compare the findings with previous scholarship and to contextualise the implications identified in the Discussion, rather than as a substitute for primary legal authority.

A temporal distinction was also maintained between current law and superseded law. The former Law of the Republic of Kazakhstan No. 370 of 2003 "On Electronic Document and Electronic Digital Signature" was considered only where necessary to understand the historical development of digital regulation and was not treated as the governing *lex lata* after the Digital Code of 2026 entered into force. This distinction was necessary to prevent conflating historical provisions and proposed forensic safeguards with current statutory requirements.

The analytical outcome of the method was therefore not a catalogue of investigative techniques, but a structured doctrinal model linking three stages of criminal proof: (1) identification of what must legally

be proved; (2) determination of how investigative information acquires evidentiary status through procedural transformation; and (3) assessment of whether the existing legal framework provides sufficiently specific safeguards when the relevant information is digital. On this basis, the study develops a hybrid evidentiary model that integrates substantive criminal-law requirements, criminal-procedural mechanisms, and digital-forensic safeguards while maintaining the distinction between existing law and proposed procedural reform.

RESULTS

Normative Structure of Proof in Human Trafficking Cases

The normative structure of proof in human trafficking proceedings in Kazakhstan is determined primarily by Article 128 of the Penal Code of the Republic of Kazakhstan, Articles 111–113 of the Criminal Procedure Code of the Republic of Kazakhstan, the Supreme Court's Normative Decree No. 7 on the application of legislation establishing liability for human trafficking, and the Law of the Republic of Kazakhstan No. 110-VIII of 5 July 2024 "On Countering Human Trafficking" (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111–113; Law on Countering Human Trafficking, 2024; Penal Code of the Republic of Kazakhstan, 2014, Art. 128; Supreme Court of the Republic of Kazakhstan, 2012). These domestic provisions operate alongside Kazakhstan's obligations under the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (Protocol to Prevent, Suppress and Punish Trafficking in Persons, 2000). Under Article 113 of the Criminal Procedure Code, criminal proceedings must establish the event and constituent elements of the offence, the identity of the person who committed it, guilt and the form of guilt, relevant motives, circumstances affecting liability, the consequences of the offence, and the nature and extent of the resulting harm (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 113). Accordingly, proof in a trafficking case cannot be reduced to showing that a person was recruited or moved. The prosecution must establish the particular form of conduct alleged under Article 128 and all additional circumstances required for the applicable legal qualification.

The objective side of trafficking under Article 128 encompasses several legally distinct forms of conduct. These include the purchase or sale of a person, other transactions concerning a person, exploitation itself, recruitment, transportation, transfer, harbouring, receipt, and other acts committed for the purpose of exploitation (Penal Code of the Republic of Kazakhstan, 2014, Art. 128(1)). The Supreme Court has clarified that the legally relevant forms of trafficking must be distinguished according to their constituent elements and that purchase, sale, or another transaction concerning a person differs doctrinally from recruitment, transportation, transfer, harbouring, receipt, and other acts performed for exploitation (Supreme Court of the Republic of Kazakhstan, 2012, para. 2). The evidentiary inquiry must therefore identify precisely what the accused is alleged to have done rather than treating trafficking as a single undifferentiated course of conduct. Purchase or sale may be reflected in payments, transfers of money, agreements, correspondence, or testimony concerning the transfer of control over a person. Recruitment may be evidenced through employment offers, communications, advertisements, victim or witness testimony, and arrangements preceding movement or exploitation. Transportation and transfer may be reconstructed from travel records, border-crossing information, tickets, accommodation records, vehicle data, or testimony, while harbouring and receipt may be demonstrated through evidence linking

the victim, offender, and location in which control or exploitation occurred. These sources are illustrative of the types of factual data capable of establishing the particular statutory conduct alleged.

The subjective side requires a more differentiated analysis. Kazakhstan's law does not support the proposition that every form of trafficking must invariably be proved through an identical "act-means-purpose" formula. The Supreme Court expressly distinguishes transactions concerning a person from recruitment, transportation, transfer, harbouring, receipt, and comparable acts. For the purchase, sale, or another transaction concerning a person, a special purpose of exploitation is not required for legal qualification; the subjective side is characterised by direct intent. By contrast, for recruitment, transportation, transfer, harbouring, receipt, and other acts directed toward exploitation, exploitative purpose constitutes a mandatory element and must be established together with direct intent (Supreme Court of the Republic of Kazakhstan, 2012, para. 2). Exploitative purpose will frequently have to be inferred from the totality of relevant circumstances, including arrangements for forced labour or sexual exploitation, restrictions imposed on the victim, instructions exchanged among participants, concealment of identity documents, distribution of proceeds, or patterns of recruitment. Motive must also be distinguished from purpose. Although motive is included among the circumstances to be proved in criminal proceedings, it does not automatically constitute a constituent element of the basic offence under Article 128 and must be assessed according to its relevance to qualification, liability, or sentencing (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 113(1)(3); Penal Code of the Republic of Kazakhstan, 2014, Art. 128).

The circumstances relating to the victim form a further component of the normative structure of proof because they may determine the applicable offence, establish qualifying circumstances, or affect the assessment of harm and protection needs. The victim's identity and age must be established because trafficking involving a minor is separately regulated under Article 135 of the Penal Code (Penal Code of the Republic of Kazakhstan, 2014, Art. 135). Other victim-related circumstances may also be legally material, including pregnancy, material or other dependence on the offender, mental disorder or helplessness, the involvement of multiple victims, and other circumstances specified in Article 128 (Penal Code of the Republic of Kazakhstan, 2014, Art. 128(2)). The Law on Countering Human Trafficking further defines a potential victim as a person in a vulnerable position resulting, *inter alia*, from material, psychological, or other dependence, minority or old age, disability, illness, unemployment, homelessness, or unsettled legal status, and establishes a formal procedure for identifying victims of trafficking (Law on Countering Human Trafficking, 2024, Arts. 1, 16). These characteristics should not, however, be treated as interchangeable with the constituent elements of every trafficking offence. Their evidentiary significance depends on the specific substantive provision relied upon by the prosecution.

Similarly, the victim's apparent consent does not necessarily exclude criminal liability. The Note to Article 128 provides that consent to exploitation does not exclude criminal liability where it was obtained through violence or threats, deception or abuse of trust, abuse of official position, material or other dependence, exploitation of mental disorder or helplessness, removal, concealment or destruction of identity documents, or other means of influence (Penal Code of the Republic of Kazakhstan, 2014, Art. 128, Note). This approach is consistent with Article 3(b) of the Palermo Protocol, under which a victim's consent to intended exploitation is irrelevant where any of the prohibited means specified in Article 3(a) have been used (Protocol to Prevent, Suppress and Punish Trafficking in Persons, 2000, Art. 3(a)–(b)).

The evidentiary inquiry must also establish the identity, role, and degree of participation of the accused and any accomplices. Article 113 of the Criminal Procedure Code requires proof of who committed the prohibited act and of that person's guilt (Criminal Procedure Code of the Republic of Kazakhstan, 2014,

Art. 113(1)(2)–(3)). Article 128 further establishes aggravated liability for circumstances including commission by a group acting by prior agreement, repetition, abuse of official position, specified transnational conduct, and commission by a criminal group (Penal Code of the Republic of Kazakhstan, 2014, Art. 128(2)–(4)). The Supreme Court further clarifies the application of the provisions concerning material or other dependence, transnational trafficking, and trafficking committed by a criminal group (Supreme Court of the Republic of Kazakhstan, 2012, paras. 16–18). Where several persons perform different functions within a trafficking scheme, the prosecution must therefore individualise the conduct attributable to each accused and establish the legal connection between that conduct and the offence charged.

The consequences of trafficking and the harm suffered by the victim constitute an additional dimension of proof. Article 113 of the Criminal Procedure Code requires the establishment of both the consequences of the criminal offence and the nature and extent of the harm caused (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 113(1)(6)–(7)). Depending on the circumstances of the case, relevant harm may include physical injury, psychological harm, deprivation of liberty, loss of earnings, forced or unpaid labour, sexual exploitation, and other material or non-material consequences. Article 128 also establishes aggravated liability where trafficking results through negligence in the death of the victim or other serious consequences (Penal Code of the Republic of Kazakhstan, 2014, Art. 128(4)). Proof of harm must therefore be connected both to the circumstances experienced by the individual victim and to the legal significance assigned to those consequences under the applicable criminal provision.

This analysis demonstrates that the normative structure of proof in trafficking proceedings is offence-specific and multi-layered. The prosecution must first identify the precise statutory form of conduct alleged and then determine which constituent elements and qualifying circumstances attach to that form. The circumstances to be proved may concern prohibited conduct, direct intent, exploitative purpose where legally required, victim-related characteristics, the identity and role of each offender, qualifying circumstances, and the consequences and harm caused (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 113; Penal Code of the Republic of Kazakhstan, 2014, Arts. 128, 135). No single category of evidence will ordinarily establish all these matters. Trafficking proceedings therefore require a multi-source evidentiary structure in which different forms of factual information corroborate one another and collectively establish the circumstances required by substantive criminal law and criminal procedure. Table 1 summarises this normative structure and its principal evidentiary implications.

Table 1 Normative Matrix of Circumstances to Be Proved in Human Trafficking Proceedings

Legal circumstances to be proved	Primary legal basis	Evidentiary significance	Illustrative evidentiary sources	Main evidentiary difficulty
Prohibited act constituting trafficking: purchase or sale, another transaction concerning a	Penal Code of the Republic of Kazakhstan (2014, Art. 128(1)); Supreme Court of the	Determines the specific statutory form of trafficking that must be established and prevents different	Victim and witness testimony; agreements; travel and border records; accommodation records; employment	Conduct may be divided among several participants, places, and stages, making the

Legal circumstances to be proved	Primary legal basis	Evidentiary significance	Illustrative evidentiary sources	Main evidentiary difficulty
person, exploitation, recruitment, transportation, transfer, harbouring, receipt, or other legally relevant conduct	Republic of Kazakhstan (2012, para. 2); Protocol to Prevent, Suppress and Punish Trafficking in Persons (2000, Art. 3)	forms of conduct from being treated as legally identical	offers; advertisements; correspondence; financial transfers; physical and documentary records	reconstruction of the complete factual sequence difficult
Direct intent and, where legally required, the purpose of exploitation	Penal Code of the Republic of Kazakhstan (2014, Art. 128(1)); Supreme Court of the Republic of Kazakhstan (2012, para. 2); Criminal Procedure Code of the Republic of Kazakhstan (2014, Art. 113(1)(3))	Distinguishes the subjective requirements applicable to different forms of trafficking	Communications between participants; instructions; arrangements for exploitation; recruitment patterns; payment records; conditions imposed on victims; testimony; circumstantial evidence	Direct evidence of intent or purpose is uncommon and may have to be inferred from a combination of circumstances
Qualifying means and circumstances, where applicable	Penal Code of the Republic of Kazakhstan (2014, Art. 128(2), Note); Supreme Court of the Republic of Kazakhstan (2012)	Determines whether conduct falls within an aggravated form of the offence and may explain how control over the victim was established or maintained	Victim and witness testimony; medical findings; communications containing threats or deception; identity documents; employment or financial records; official records	Coercion or dependency may be psychological, economic, relational, or indirect and may leave no obvious physical trace
Identity, age, and legally relevant characteristics of the victim	Penal Code of the Republic of Kazakhstan (2014, Arts. 128, 135); Criminal Procedure Code of the Republic of	Determines the applicable offence and may establish qualifying circumstances or particular	Identity and birth records; migration documents; official databases; testimony; social-service records; medical or	Victims may lack reliable documents, use different identities, have irregular migration status,

Legal circumstances to be proved	Primary legal basis	Evidentiary significance	Illustrative evidentiary sources	Main evidentiary difficulty
	Kazakhstan (2014, Art. 113); Law on Countering Human Trafficking (2024, Arts. 1, 16); Protocol to Prevent, Suppress and Punish Trafficking in Persons (2000, Art. 3(c)–(d))	protection requirements	psychological assessments	or be unable or unwilling to provide complete information
Victim dependence, vulnerability, and relationship with the offender, where legally relevant	Penal Code of the Republic of Kazakhstan (2014, Art. 128(2), Note); Law on Countering Human Trafficking (2024, Art. 1); Supreme Court of the Republic of Kazakhstan (2012, para. 16)	May constitute a qualifying circumstance, explain the means of control, or affect identification and protection of the victim	Family, employment, housing, migration, financial, and social-service records; testimony; evidence of economic or other dependence	Vulnerability is contextual and may arise from several overlapping circumstances
Identity, role, participation, and guilt of each offender or accomplice	Criminal Procedure Code of the Republic of Kazakhstan (2014, Art. 113(1)(2)–(5)); Penal Code of the Republic of Kazakhstan (2014, Art. 128(2), (4))	Individualises criminal responsibility and connects each accused with the conduct charged	Testimony; communications; banking and financial records; travel records; surveillance materials; documents; records linking persons with premises, accounts, vehicles, or transactions	Different functions may be divided among multiple participants and jurisdictions
Transnational or organised	Penal Code of the Republic of	Determines enhanced	Border records; travel and migration	Evidence may be distributed across

Legal circumstances to be proved	Primary legal basis	Evidentiary significance	Illustrative evidentiary sources	Main evidentiary difficulty
circumstances, where charged	Kazakhstan (2014, Art. 128(3)–(4)); Supreme Court of the Republic of Kazakhstan (2012, paras. 17–18)	qualification where trafficking involves export, import, transit, or commission by a criminal group	documents; international financial transactions; communications; evidence obtained through international cooperation	jurisdictions and controlled by different public or private entities
Consequences and nature and extent of harm	Criminal Procedure Code of the Republic of Kazakhstan (2014, Art. 113(1)(6)–(7)); Penal Code of the Republic of Kazakhstan (2014, Art. 128(4))	Relevant to qualification, compensation, sentencing, and aggravated liability	Medical and psychological assessments; victim testimony; financial-loss calculations; employment records; evidence of deprivation of liberty or unpaid labour; expert findings	Psychological and non-material harm may be cumulative, long-term, and difficult to quantify
Lawfulness and procedural admissibility of factual data	Criminal Procedure Code of the Republic of Kazakhstan (2014, Arts. 111–113)	Determines whether information collected during investigation can perform an evidentiary function in criminal proceedings	Protocols of procedural actions; testimony; expert conclusions; material evidence; documents and other lawfully obtained factual data	Relevant information may lose evidentiary value where obtained or introduced contrary to mandatory procedural requirements

Note. Compiled by the author from the Penal Code of the Republic of Kazakhstan (2014, Arts. 128, 135), the Criminal Procedure Code of the Republic of Kazakhstan (2014, Arts. 111–113), the Supreme Court of the Republic of Kazakhstan (2012, paras. 2, 16–18), the Law on Countering Human Trafficking (2024, Arts. 1, 16), and the Protocol to Prevent, Suppress and Punish Trafficking in Persons (2000, Art. 3).

The normative matrix demonstrates that identifying the circumstances to be proved constitutes only the first stage of the evidentiary process. Investigators may obtain information concerning recruitment, transportation, control, exploitation, offenders, and victims through operational-investigative activities, but the existence of relevant information does not by itself determine its procedural status as evidence. The next analytical question is therefore procedural rather than substantive: through what legal process does information generated by operational-investigative measures acquire the status and evidentiary value necessary for use in proving a criminal case? Answering this question requires distinguishing among operational-investigative information, criminal-procedural investigative actions,

and factual data that satisfy the requirements governing evidence under the Criminal Procedure Code. The following section examines this process of procedural transformation.

Evidentiary Value of Operational-Investigative Measures

The identification of the circumstances that must be proved in a human trafficking case does not, by itself, resolve the evidentiary problem. Investigators may obtain information concerning recruitment, transportation, places of exploitation, communications among offenders, financial transactions, or the identity and location of victims without every item of that information immediately acquiring the legal status of evidence. Kazakhstan's legal framework distinguishes between information generated through operational-investigative activity and factual data incorporated into criminal proceedings through procedural forms recognised by the Criminal Procedure Code. The central issue is therefore not simply which investigative technique produces information, but when and through what legal process that information acquires evidentiary value. This distinction is particularly relevant in trafficking proceedings because operational-investigative measures may identify persons, locations, communications, and other circumstances before those findings are incorporated into formal criminal proceedings (Law on Operational Investigations, 1994, Arts. 2, 10–11; Supreme Court of the Republic of Kazakhstan, 2020, paras. 3–5).

At the first level, operational-investigative activity primarily performs detection, prevention, identification, and intelligence functions. The Law on Operational Investigations defines operational-investigative activity as a system of overt and covert operational measures carried out by authorised bodies to protect individuals, society, and the state from criminal infringements. Its statutory tasks include detecting, preventing, suppressing, and disclosing criminal offences; identifying persons involved in criminal activity; searching for persons; and obtaining information relevant to criminal conduct (Law on Operational Investigations, 1994, Arts. 1–2). In trafficking investigations, such measures may therefore identify victims and suspects, premises associated with recruitment or exploitation, routes of movement, communication channels, and relationships among participants. The information produced may take the form of documents, items, materials, operational records, or information retained in operational information systems. Article 14-1 expressly permits authorised bodies to create and use operational records and information systems for collecting, systematising, verifying, and evaluating the results of operational-investigative activity (Law on Operational Investigations, 1994, Art. 14-1).

The existence of operational information, however, must be distinguished from its evidentiary use. Article 14(1) of the Law on Operational Investigations provides that materials obtained through operational-investigative activity may be used in preparing and conducting investigative actions and may also be used in proving criminal cases, subject to verification in accordance with criminal-procedure rules governing the collection, examination, and evaluation of evidence (Law on Operational Investigations, 1994, Art. 14(1)). The Supreme Court has confirmed this distinction, explaining that operational-investigative materials may be used in proving only after compliance with the relevant criminal-procedure requirements. It further clarifies that materials obtained in accordance with operational-investigative legislation and containing factual data on unlawful acts may qualify as documents and be used as evidence under Article 120 of the Criminal Procedure Code (Supreme Court of the Republic of Kazakhstan, 2020, paras. 3–4). Operational origin, therefore, neither automatically excludes information from evidentiary use nor automatically confers upon it the status of evidence capable of judicial use. Its evidentiary significance depends on the legal route through which it is verified and incorporated into criminal proceedings.

The Criminal Procedure Code provides the second level of this process. Article 121 defines proof as the collection, examination, evaluation, and use of evidence for establishing circumstances relevant to the lawful, reasonable, and fair resolution of a criminal case. Article 122 provides that evidence is collected during pre-trial investigation and trial through procedural actions established by the Code, including the detection, fixation, and seizure of evidence (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 121–122). Accordingly, when operational information identifies a relevant person, place, communication, object, document, or factual circumstance, criminal-procedural mechanisms may subsequently be used to obtain, verify, and formally record that information in a legally recognised manner. Depending on the nature of the information, these mechanisms may include interrogation, inspection, search, seizure, presentation and examination of documents, expert examination, investigative experiment, or other procedural actions provided for by the Code.

The legal significance of procedural form is further reflected in Articles 119 and 123 of the Criminal Procedure Code. Article 119 recognises factual data contained in properly prepared protocols of procedural actions, including information established during inspections, seizures, searches, presentations of documents, investigative experiments, and examinations of the results of covert investigative actions (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 119). Article 123 regulates the fixation of factual data in procedural protocols and establishes requirements concerning the recording and preservation of such information (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 123). Procedural documentation, therefore, serves more than an administrative function: it records how factual data were obtained, preserved, and introduced into the criminal case, thereby making their procedural origin subject to subsequent examination.

The Code recognises more than one procedural route through which operational materials may acquire evidentiary significance. Article 120(2) expressly provides that materials containing factual data on unlawful acts and obtained in compliance with legislation governing operational-investigative activity constitute documents and may be used as evidence in criminal proceedings (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 120(2)). Article 120 also encompasses materials containing computer information, photographs, films, sound recordings, and video recordings when obtained, requested, or submitted in the manner prescribed by criminal-procedure law (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 120). Where an object or document possesses the statutory characteristics of material evidence, it may instead be treated under Article 118 (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 118). Consequently, procedural transformation should not be understood as a single mechanical conversion process. The appropriate route depends on the nature of the factual information and the evidentiary category into which it is lawfully incorporated.

Covert investigative actions require separate treatment because they form part of criminal procedure itself and are governed by a specific statutory regime under Chapter 30 of the Criminal Procedure Code. The Supreme Court expressly requires courts to distinguish covert investigative actions carried out within a criminal case from operational-search measures conducted under the Law on Operational Investigations (Supreme Court of the Republic of Kazakhstan, 2020, para. 3). Covert investigative actions are conducted during pre-trial proceedings to establish circumstances subject to proof without prior notification of affected persons and, as a rule, where the relevant information cannot be obtained through ordinary investigative actions (Supreme Court of the Republic of Kazakhstan, 2020, paras. 1–2). Articles 231–240 of the Criminal Procedure Code establish the grounds, conditions, authorisation procedures, duration, examination, preservation, and evidentiary treatment of the results of such actions (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 231–240).

Within this statutory framework, Article 237 requires materials obtained through covert investigative actions to be transmitted to the body conducting the pre-trial investigation. Article 238 regulates their examination and requires a protocol to be prepared, with the participation of a specialist where necessary. Relevant factual data and materials are attached to the protocol (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 237–238). Article 239 then governs the evaluation and use of the results in proving. Protocols recording the examination of covert investigative actions, sound and image recordings, photographs, materials obtained through scientific and technical means, and seized objects and documents or their copies may be used alongside evidence obtained through other investigative actions (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 239).

The evidentiary significance of covert investigative material, therefore, depends not merely on the existence of a recording or other factual information but on compliance with the statutory requirements governing authorisation, conduct, transmission, examination, fixation, and evaluation. The Supreme Court similarly emphasises that covert investigative actions must be distinguished from operational measures and conducted only within the limits of the authorised order; information obtained outside those limits may not be recognised as admissible evidence (Supreme Court of the Republic of Kazakhstan, 2020, paras. 5, 12). This consequence is particularly explicit for urgent covert investigative actions. Under Article 235, an urgent covert action may commence without prior judicial authorisation only under conditions prescribed by law and subject to subsequent judicial review. If the investigating judge finds the action unjustified, the action must be terminated, and its results cannot be used as evidence (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 235(2); Supreme Court of the Republic of Kazakhstan, 2020, paras. 18–20).

At the third level, information lawfully incorporated into criminal proceedings remains subject to evidentiary examination and evaluation. Article 111 defines evidence as lawfully obtained factual data through which competent criminal-procedure authorities establish the existence or absence of a criminal offence, the involvement and guilt or innocence of the suspect or accused, and other circumstances relevant to the proper resolution of the case (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 111). Article 124 requires collected evidence to be comprehensively and objectively examined through analysis, comparison with other evidence, verification of its source, and, where necessary, collection of additional evidence (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 124). Article 125 subsequently requires each item of evidence to be evaluated in terms of relevance, admissibility, and reliability, while the totality of the evidence must also be evaluated for sufficiency (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 125).

Admissibility consequently functions as an important procedural filter between investigative information and evidence capable of supporting criminal adjudication. Article 125 provides that evidence is admissible if obtained in accordance with the procedure established by the Criminal Procedure Code (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 125). Article 112 establishes the consequences of non-compliance. Factual data obtained through violations of criminal-procedure requirements that affect or could affect their reliability must be recognised as inadmissible. This includes, among other circumstances, evidence obtained by an unauthorised person, through substantial violations of procedural requirements, or from an unknown or unverifiable source (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 112). Evidence obtained in violation of criminal procedure law cannot serve as the basis for prosecution or be used to establish the circumstances subject to proof under Article 113 (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 112(4), 113).

The relationship among these three levels can therefore be conceptualised as a process of procedural transformation. Operational-investigative information performs a detection and orientation function and may reveal facts relevant to a future or ongoing prosecution. Criminal procedural mechanisms provide the legally regulated means by which relevant information is collected, verified, fixed, seized, or otherwise incorporated into the case. The resulting factual data may then function as evidence within one of the evidentiary forms recognised by the Criminal Procedure Code and remain subject to examination for relevance, admissibility, reliability, and, collectively, sufficiency (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111–125; Supreme Court of the Republic of Kazakhstan, 2020, paras. 3–4). Table 2 summarises this procedural transformation and the legal status associated with each stage.

Tabel 2 Procedural Transformation of Investigative Information into Admissible Evidence

Stage	Primary legal basis	Primary function	Illustrative output	Route into criminal proceedings	Evidentiary status
Operational-investigative measures	Law on Operational Investigations (1994, Arts. 2, 10–11, 14, 14-1); Supreme Court of the Republic of Kazakhstan (2020, paras. 3–4)	Detection and prevention of criminal activity; identification and location of victims and suspects; identification of premises, routes, communications, relationships, and other operationally relevant information	Operational records; reports; surveillance information; information contained in operational databases and information systems; other authorised operational materials	Materials used in proving must be verified in accordance with criminal-procedure rules governing collection, examination, and evaluation and may subsequently be incorporated as documents, material evidence, or through another recognised procedural route	Have potential evidentiary significance but do not acquire judicial evidentiary status solely because they were obtained through operational-investigative activity
Criminal-procedural investigative actions	Criminal Procedure Code of the Republic of Kazakhstan	Collection, verification, fixation, and seizure of facts relevant to the	Interrogation testimony and protocols; inspection records; search and	Information is obtained or verified through a procedural action	May constitute evidence when obtained, fixed, preserved, and introduced in

Stage	Primary legal basis	Primary function	Illustrative output	Route into criminal proceedings	Evidentiary status
	(2014, Arts. 111, 118–123)	circumstances subject to proof	seizure records; investigative-experiment protocols; documents; material objects; expert and specialist conclusions	prescribed by the CPC and incorporated into one of the evidentiary forms recognised by criminal-procedure law	accordance with the CPC
Covert investigative actions	Criminal Procedure Code of the Republic of Kazakhstan (2014, Arts. 231–240); Supreme Court of the Republic of Kazakhstan (2020, paras. 1–5, 12, 18–20)	Covert acquisition and documentation of communications, conduct, contacts, locations, objects, or other circumstances where statutory grounds for covert investigation exist	Protocols; sound and image recordings; photographs; information recorded through scientific and technical means; seized objects; documents or copies	Results are transmitted to the pre-trial investigation body under Article 237, examined and recorded under Article 238, and subsequently evaluated and used under Article 239	May be used in proving when statutory requirements concerning grounds, authorisation, conduct, examination, fixation, and evaluation are satisfied; unlawfully obtained results may be inadmissible
Evidence capable of judicial use	Criminal Procedure Code of the Republic of Kazakhstan (2014, Arts. 111–125)	Establishment of guilt or innocence, legal qualification, harm, and other circumstances subject to proof	Testimony; expert and specialist conclusions; material evidence; protocols of procedural actions; documents and other factual data recognised by the CPC	Evidence is examined, source-verified, compared, and evaluated within criminal proceedings	Capable of supporting judicial findings when relevant, admissible, and reliable; the totality of the evidence must also be sufficient

Note. Compiled by the author from the Law on Operational Investigations (1994, Arts. 2, 10–11, 14, 14-1), the Criminal Procedure Code of the Republic of Kazakhstan (2014, Arts. 111–125, 231–240), and the Supreme Court of the Republic of Kazakhstan (2020, paras. 1–5, 12, 18–20).

The procedural matrix generates four principal findings concerning the evidentiary architecture of human trafficking proceedings. First, operational-investigative information and evidence capable of judicial use are not legally equivalent. Operational materials may contain substantial factual information and may be used in proving, but their evidentiary use is conditioned upon compliance with criminal-procedure requirements concerning verification and incorporation into proceedings (Law on Operational Investigations, 1994, Art. 14(1); Supreme Court of the Republic of Kazakhstan, 2020, para. 4). The distinction therefore concerns legal status and procedural treatment rather than merely informational content. The same underlying information may initially serve an operational function and subsequently acquire evidentiary significance after it has been lawfully verified and introduced through an evidentiary form recognised by the Criminal Procedure Code.

Second, the decisive stage is procedural transformation. Criminal procedure does not conceptualise proof as the mere accumulation of information. Article 121 defines proof through the processes of collection, examination, evaluation, and use, while Articles 122–125 regulate how factual information is obtained, fixed, examined, and evaluated (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 121–125). Operational material may be verified and incorporated as a document under Article 120; an object may qualify as material evidence under Article 118; relevant facts may be reproduced or independently established through interrogation, inspection, search, seizure, or another investigative action; and covert-investigation results follow the specific procedural route established by Articles 237–239 (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 118–120, 237–239). The evidentiary system is therefore functional rather than mechanical: the decisive question is whether factual information has entered the criminal process through a legally recognised route capable of preserving and verifying its source and integrity.

Third, procedural transformation may fail at several stages. Defects concerning legal authorisation, the competence of the person conducting an investigative action, the manner in which information is obtained, procedural fixation, identification of the source, or subsequent examination may affect admissibility or reliability. Article 112 excludes factual data obtained through specified procedural violations, while Article 125 requires each item of evidence to be separately evaluated for admissibility and reliability (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 112, 125). The Supreme Court likewise confirms that information obtained through a covert investigative action beyond the limits of the authorised order may not be recognised as admissible evidence (Supreme Court of the Republic of Kazakhstan, 2020, para. 12). Investigative success in identifying relevant facts therefore does not necessarily amount to evidentiary success; those facts must survive the procedural requirements governing their movement from investigation to proof.

Fourth, this distinction becomes especially consequential when the underlying source is digital. Digital information may be copied, modified, deleted, dynamically generated, distributed across devices and servers, or retained by third-party service providers. Accordingly, the procedural questions already identified—how information is lawfully obtained, fixed, attributed, preserved, examined, and verified—become particularly important when investigative material consists of screenshots, screen recordings, messaging data, social-media content, metadata, server information, or other computer-derived data. Kazakhstan's Criminal Procedure Code expressly recognises computer information, photographs, sound recordings, video recordings, and other technically recorded materials as potentially relevant evidentiary

forms (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 120). The remaining question is therefore whether the existing procedural framework provides sufficiently specific safeguards to establish the authenticity, integrity, provenance, attribution, and admissibility of such digital material.

This finding leads to the next stage of the analysis. Once the distinction between operational information and evidence capable of judicial use has been established, it becomes necessary to examine whether Kazakhstan's existing evidentiary rules adequately address the particular characteristics of digital information. The following section, therefore, analyses the current legal treatment of digital evidence, identifies areas in which the law provides only general rather than technology-specific requirements, and distinguishes existing legal requirements (*lex lata*) from additional procedural safeguards proposed for future regulation (*lex ferenda*).

Legal Gaps in the Admissibility and Preservation of Digital Evidence

The increasing use of digital platforms in recruitment, communication, control, payment, and coordination has made electronically stored information increasingly important to the evidentiary architecture of human trafficking investigations. The relevant legal question is not merely whether digital information can be factually relevant, but how such information fits within the evidentiary categories and procedural requirements established by Kazakhstan law. The current framework consists primarily of the Criminal Procedure Code of the Republic of Kazakhstan and the Digital Code of the Republic of Kazakhstan No. 255-VIII of 9 January 2026 (Criminal Procedure Code of the Republic of Kazakhstan, 2014; Digital Code of the Republic of Kazakhstan, 2026). The Digital Code now regulates electronic documents, digital documents, digital data, and electronic digital signatures and replaced the earlier Law "On Electronic Document and Electronic Digital Signature" (Digital Code of the Republic of Kazakhstan, 2026, Arts. 49–50, 62–64; Law on Electronic Document and Electronic Digital Signature, 2003). These developments provide a broader legal framework for digital information, but they do not by themselves establish a comprehensive criminal-procedural regime for every form of digital evidence that may arise in trafficking proceedings.

The current *lex lata* does not establish "digital evidence" or "electronic evidence" as a separate and autonomous category of evidence under the Criminal Procedure Code. Instead, digital material is accommodated within existing evidentiary categories. Article 111 defines evidence as lawfully obtained factual data and identifies the recognised evidentiary forms, including testimony, expert and specialist conclusions, material evidence, protocols of procedural actions, and documents (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 111). Article 120 provides that documents may contain information recorded in written or other forms and expressly encompasses materials containing computer information, photographs, filming, sound recordings, and video recordings when obtained, requested, or presented in accordance with Article 122 (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 120). Objects and documents possessing the statutory characteristics specified in Article 118 may also be recognised as material evidence (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 118). The Code further recognises information submitted in electronic form within the evidentiary collection process (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 122).

The Digital Code complements this framework but serves a different regulatory function. Article 49 defines an electronic digital signature as a digital record confirming the authenticity, ownership, and

immutability of the content of an electronic document. Article 50 regulates the means for creating and verifying electronic digital signatures. Article 62 recognises a digital record as an electronic document whose authenticity, ownership, and immutability are confirmed by an electronic digital signature, while Articles 63 and 64 separately regulate digital documents and digital data (Digital Code of the Republic of Kazakhstan, 2026, Arts. 49–50, 62–64). Accordingly, Kazakhstan law already recognises multiple legally significant forms of digital information. Their use as criminal evidence, however, remains governed predominantly by the general evidentiary categories and procedural requirements of the Criminal Procedure Code rather than by a unified criminal-procedural category of “digital evidence.”

This general evidentiary framework can accommodate screenshots and screen recordings, but it does not establish a dedicated authentication regime for such materials. A screenshot may potentially fall within computer information, photography, or another documentary form recognised by Article 120, while a screen recording may be treated as computer information or a video recording (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 120). The Code also authorises the use of photography, filming, sound and video recording, and other scientific and technical means in investigative actions. Where such means are used, the protocol must identify the scientific and technical means, the conditions and procedures of their use, the objects to which they were applied, and the results obtained (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 197, 199).

These provisions constitute the applicable *lex lata* and indicate that visual or audiovisual captures are not inherently excluded from the evidentiary process. The regulatory gap is more specific: the Criminal Procedure Code does not prescribe a uniform authentication procedure uniquely applicable to screenshots of webpages or recordings of online sessions. It does not, for example, generally require every such capture to preserve the complete URL, page source, browser environment, capture timestamp, device configuration, or a cryptographic hash value. Consequently, the evidentiary problem concerns the ability to demonstrate the capture's source, completeness, integrity, temporal context, and relationship with the underlying online content. Recommended practices such as documenting the original digital source, maintaining an auditable preservation record, and using cryptographic hashes to support integrity verification are well established in digital-evidence preservation guidance, but these practices should be understood as recommended forensic safeguards rather than existing requirements of Kazakhstan criminal-procedure law (Guttman et al., 2022; Kent et al., 2006).

The treatment of metadata reveals a similar distinction between general legal recognition and technology-specific procedural regulation. The Digital Code recognises digital data and establishes mechanisms for verifying authenticity and integrity in particular contexts, most notably those involving electronic documents certified by electronic digital signatures (Digital Code of the Republic of Kazakhstan, 2026, Arts. 49, 62–64). The Criminal Procedure Code, however, does not establish “metadata” as an autonomous evidentiary category or prescribe a comprehensive procedure specifically governing the extraction and preservation of file-system metadata, EXIF data, communication metadata, application metadata, server headers, account identifiers, or comparable technical attributes. Such information may nevertheless fall within computer information or be examined through the participation of a specialist or expert under the general evidentiary framework (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 80, 111, 120).

The resulting gap is therefore not that metadata is legally incapable of acquiring evidentiary significance. Rather, the Criminal Procedure Code lacks a uniform, technology-specific protocol governing how metadata should be acquired, preserved, documented, and verified to demonstrate its provenance and subsequent integrity. This distinction is important because ordinary access, copying, conversion, or

export of digital material may alter certain technical attributes. Digital-evidence preservation guidance accordingly emphasises documentation of the original source, preservation history, integrity verification, and controlled handling of digital files (Guttman et al., 2022). Applied to Kazakhstan, these measures constitute *lex ferenda*-oriented safeguards that could operationalise existing requirements of reliability and verification rather than rules that should be presented as already mandatory under the Code.

Social media and messenger data can likewise be incorporated into the existing evidentiary framework. Messages, account information, images, video files, payment instructions, and other communications may qualify as documents containing computer information when lawfully obtained and incorporated into criminal proceedings (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 120). Chapter 30 of the Criminal Procedure Code provides more specific mechanisms for covert acquisition of certain forms of digitally transmitted or stored information. Article 231 includes covert interception and removal of information transmitted through telecommunications networks, covert obtaining of information concerning connections between subscribers or subscriber devices, and covert collection of information from computers, servers, and other devices (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 231). Articles 232–239 regulate the statutory conditions, authorisation, transmission, examination, evaluation, and evidentiary use of the results of covert investigative actions (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 232–239).

These provisions constitute a significant part of Kazakhstan's *lex lata* for digitally mediated investigation. They do not, however, eliminate the separate evidentiary problem of attribution. The existence of a message, profile, username, or account does not by itself establish that the accused created, controlled, or transmitted the material. An account may be shared, fictitious, compromised, or operated through devices used by several persons. The applicable legal standard, therefore, remains one of examination, reliability, and corroboration under the general evidentiary rules (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 124–125). Technical identifiers, subscriber information, device records, connection information, communications, and other independently obtained factual data may therefore be relevant to establishing the connection between a digital identity and a particular person.

A related problem arises with saved HTML files, archived webpages, and website replicas. Under the current framework, saved online content may potentially fall within Article 120 as a document containing computer information, provided that it has been obtained, requested, or presented in accordance with the procedural rules governing evidence (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 120, 122). The Code also permits documents and copies to perform evidentiary functions in specified procedural contexts, including materials generated through covert investigative actions (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 120, 239). It would therefore be inaccurate to suggest that Kazakhstan law invariably requires a technically unique digital “original” before digital material can be used in proving.

At the same time, the Criminal Procedure Code does not establish a comprehensive rule defining what constitutes an original digital object, when a forensic copy is evidentially equivalent to its source, or what technical process is required to establish that an archived webpage accurately corresponds to the version available at a legally relevant time. A saved HTML file or website replica may preserve visible content while omitting server-side information, dynamically generated elements, access logs, publication history, or other contextual data. The principal evidentiary risk is consequently the uncertain relationship between the preserved representation and the original digital environment. Documentation of the source, acquisition process, preservation method, and integrity of the resulting copy would strengthen

verifiability, but such practices should again be characterised as recommended safeguards rather than current statutory requirements (Guttman et al., 2022; Kent et al., 2006).

Digital devices and storage media are more directly accommodated within existing criminal-procedural mechanisms. Devices or storage media may qualify as material evidence where they possess the characteristics established under Article 118, and scientific and technical means may be used during investigative actions for detecting, fixing, and seizing traces and material evidence (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 118, 197). Article 199 additionally requires that investigative protocols identify the scientific and technical means used, the conditions and procedures for their application, the relevant objects, and the results obtained (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 199).

Article 245 provides an even more specific rule for the covert collection of information from computers, servers, and other devices used for collecting, processing, accumulating, and storing information. The provision requires the resulting information to be recorded on an appropriate material carrier, which must be packaged, sealed, certified by the authorised official, and transferred to the investigator or interrogating officer (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 245). These rules demonstrate that Kazakhstan's criminal procedure already contains specific integrity-oriented safeguards for certain computer-derived information.

The limitation is therefore not an absolute absence of preservation requirements. Rather, the existing requirements apply within particular procedural contexts and do not constitute a uniform digital chain-of-custody regime governing every form of digital evidence from initial acquisition through forensic duplication, examination, storage, transfer, and courtroom presentation. Digital-forensic guidance recommends maintaining a clearly documented chain of custody, preserving original data, examining copies where practicable, documenting tools and actions, and using cryptographic hashes to support integrity verification (Guttman et al., 2022; Kent et al., 2006). Such measures provide a useful basis for *lex ferenda*, but should not be conflated with the current requirements of Articles 118, 197, 199, or 245 of the Criminal Procedure Code.

The cross-border character of human trafficking creates an additional challenge where relevant digital information is controlled by a foreign platform, service provider, or server operator. Kazakhstan's Criminal Procedure Code contains a statutory framework for international cooperation and legal assistance in criminal proceedings, while the Law on Countering Human Trafficking expressly addresses international cooperation in trafficking-related cases (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Section 12; Law on Countering Human Trafficking, 2024, Art. 12). Article 12(3) of the latter provides that international legal assistance in criminal cases involving trafficking-related offences is conducted in accordance with international treaties to which Kazakhstan is a party and, where such treaties are absent, on the basis of reciprocity under the procedure established by the Criminal Procedure Code (Law on Countering Human Trafficking, 2024, Art. 12(3)).

Foreign-held digital information is therefore not legally inaccessible merely because the relevant data are located outside Kazakhstan. The remaining problem concerns the interaction between conventional international legal-assistance procedures and the temporal and technical characteristics of digital information. Platform data may be altered or deleted, records may be subject to limited retention periods, and foreign authorities or service providers may apply different disclosure, certification, privacy, preservation, or authentication procedures. The current framework establishes a legal route for international cooperation but does not itself prescribe a harmonised, technology-specific procedure for the rapid preservation and forensic authentication of all foreign-hosted platform or server data. Best-

practice approaches to digital evidence held by third-party or remote service providers similarly emphasise preservation, documentation of provenance, and continuity of handling, illustrating the type of procedural safeguards that may be considered in future regulatory development.

The analysis, therefore, reveals an important distinction between legal recognition and procedural specificity. Kazakhstan law already recognises computer information, electronic documents, digital data, photographs, audio and video recordings, and information acquired from computers and servers through specified procedural mechanisms (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111, 118, 120, 231, 245; Digital Code of the Republic of Kazakhstan, 2026, Arts. 49, 62–64). It also provides general requirements concerning lawful acquisition, procedural fixation, examination, preservation, admissibility, and evidentiary evaluation. The principal legal problem should therefore not be characterised as the complete absence of regulation of digital material. More precisely, the relevant provisions remain distributed across general evidentiary rules, covert-investigative provisions, and digital legislation, and do not constitute a unified criminal-procedural framework that specifically addresses authenticity, integrity, provenance, attribution, preservation, and reproducibility across the heterogeneous forms of digital evidence relevant to trafficking investigations.

This distinction is essential for formulating *lex ferenda*. Technical practices such as preserving source information and capture timestamps, documenting devices and software used, creating forensic copies, calculating cryptographic hash values, preserving relevant metadata, maintaining a documented chain of custody, and using validated forensic procedures should not be presented as if each were already expressly mandated by Kazakhstan's Criminal Procedure Code. Such techniques are better conceptualised as recommended procedural safeguards that operationalise the Code's existing requirements for lawful collection, fixation, verification, admissibility, and reliability when evidence is digital, reproducible, and susceptible to alteration (Guttman et al., 2022; Kent et al., 2006). Table 3, therefore, distinguishes the current legal position from the principal evidentiary risks and the additional safeguards proposed by this study.

Tabel 3 Current Legal Position, Admissibility Risks, and Recommended Safeguards for Digital Evidence

Type of digital evidence	Evidentiary relevance	Current legal position (<i>lex lata</i>)	Main admissibility risk	Recommended procedural safeguard (<i>lex ferenda</i>)
Screenshots and screen recordings	May preserve online recruitment advertisements, communications, threats, employment offers, account information, and exploitation-related content	Computer information, photographs, filming, sound recordings, and video recordings may enter the evidentiary process under the general documentary and procedural rules (Criminal Procedure Code of the Republic of Kazakhstan, 2014,	Authenticity; incomplete context; uncertain source, URL, or capture time; post-capture alteration; difficulty establishing authorship or correspondence	Document source/URL, capture date and time, device and software used, sequence of acquisition, and relevant account context; preserve accessible source data; generate integrity values; retain an

Type of digital evidence	Evidentiary relevance	Current legal position (<i>lex lata</i>)	Main admissibility risk	Recommended procedural safeguard (<i>lex ferenda</i>)
	displayed at a particular time	Arts. 120, 122–125, 199). No separate statutory category specifically governs screenshot evidence	with server-side content	auditable acquisition and preservation record (Guttman et al., 2022; Kent et al., 2006)
Metadata and technical attributes	May assist in establishing creation or modification information, device or account links, location, communication history, transmission information, and provenance	Metadata may fall within computer information subject to the CPC's general evidentiary regime. Digital Code provisions regulate authenticity and integrity principally in defined electronic-document and digital-data contexts (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111, 120; Digital Code of the Republic of Kazakhstan, 2026, Arts. 49, 62–64)	Metadata may be altered during copying, access, export, or conversion; provenance may be uncertain; isolated metadata may not establish attribution	Preserve source data before substantive examination; use documented forensic extraction methods; record tools and procedures; calculate integrity values where appropriate; maintain preservation and examination records (Guttman et al., 2022; Kent et al., 2006)
Social-media and messenger data	May establish recruitment, control, threats, payment arrangements, relationships among participants, locations, and communications relevant to exploitative conduct or purpose	May qualify as documents containing computer information under Article 120; Chapter 30 provides mechanisms for interception, subscriber/device information, and covert acquisition from computers and servers where statutory conditions are met (Criminal Procedure Code of the Republic of	Uncertain account ownership; shared or compromised accounts; manipulated exports; incomplete conversation context; difficulty connecting an online identity to an accused person	Corroborate attribution through subscriber/device information, account identifiers, connection records where lawfully obtainable, communication patterns, and independent evidence; preserve relevant contextual conversation data

Type of digital evidence	Evidentiary relevance	Current legal position (<i>lex lata</i>)	Main admissibility risk	Recommended procedural safeguard (<i>lex ferenda</i>)
		Kazakhstan, 2014, Arts. 120, 231–245)		
Saved HTML pages, archived webpages, and website replicas	May preserve recruitment pages, advertisements, profiles, contact information, and online material that may later be altered or removed	Saved online material may potentially fall within computer information or documentary evidence under Articles 120 and 122; the CPC permits documents and copies in specified contexts but does not establish a general forensic definition of digital originality (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 120, 122, 239)	Failure to preserve server-side information, dynamic content, publication history, original timestamps, or platform data; disputed correspondence between a copy and its source environment	Document source/URL, acquisition date and time, method and tools used; preserve available source material and relevant context; record integrity values; corroborate with provider or server records where available (Guttman et al., 2022)
Digital devices and storage media	May contain messages, photographs, files, location information, deleted data, account information, and other evidence linking victims, offenders, and trafficking activity	Devices may qualify as material evidence under Article 118; Articles 197 and 199 regulate technical means and procedural documentation; Article 245 requires computer/server-derived information obtained covertly to be recorded on a carrier, packaged, sealed, certified, and transferred (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 118, 197, 199, 245)	Data may be altered by ordinary use, seizure, access, examination, or copying; later examination may fail to reconstruct the original state	Preserve original data; create forensic copies where appropriate; use write-protection techniques where applicable; calculate and record integrity values; document seizure, access, transfer, storage, and examination (Guttman et al., 2022; Kent et al., 2006)

Type of digital evidence	Evidentiary relevance	Current legal position (<i>lex lata</i>)	Main admissibility risk	Recommended procedural safeguard (<i>lex ferenda</i>)
Foreign platform or server data	May establish account registration, connection history, communications, payments, platform activity, user information, deleted content, or other relevant records controlled abroad	International legal assistance is available under the CPC's international-cooperation framework and specifically for trafficking-related offences through Article 12(3) of the Law on Countering Human Trafficking (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Section 12; Law on Countering Human Trafficking, 2024, Art. 12(3))	Delay; deletion or expiration before acquisition; divergent foreign procedures; incomplete certification; differing privacy or evidentiary rules; difficulty establishing provenance and continuity after transfer	Develop rapid preservation mechanisms followed by formal legal-assistance procedures; specify requested technical and contextual information; obtain provider or competent-authority documentation supporting provenance; document receipt and subsequent handling; promote interoperable cross-border preservation and authentication standards

Note. Compiled by the author from the Criminal Procedure Code of the Republic of Kazakhstan (2014, Arts. 111–125, 197, 199, 231–245), the Digital Code of the Republic of Kazakhstan (2026, Arts. 49–50, 62–64), the Law on Countering Human Trafficking (2024, Art. 12), and digital-evidence preservation guidance developed by Guttman et al. (2022) and Kent et al. (2006). The final column presents recommended safeguards (*lex ferenda*) and should not be interpreted as a statement of existing mandatory law in Kazakhstan.

Four patterns emerge from the distinction between the current legal framework and the additional procedural safeguards identified in Table 3. First, there is a classification gap. The Criminal Procedure Code is sufficiently broad to accommodate computer information and other digitally recorded material within existing evidentiary categories, but it does not establish digital evidence as a coherent, autonomous category accompanied by procedural rules tailored to its technical characteristics (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111, 118, 120). Screenshots, metadata, messaging data, archived webpages, device-derived information, and server data may therefore enter proceedings through different doctrinal routes even though they raise related questions concerning authenticity, integrity, provenance, and attribution.

Second, there is an authentication gap. Kazakhstan's Digital Code establishes comparatively specific authentication and integrity mechanisms for a particular class of digital material: electronic documents associated with electronic digital signatures. An electronic digital signature confirms authenticity, ownership, and immutability under the conditions prescribed by the Code, while electronic documents

complying with Article 62 receive legal recognition (Digital Code of the Republic of Kazakhstan, 2026, Arts. 49, 62). These mechanisms do not automatically resolve authentication problems associated with ordinary web content, unsigned messages, screenshots, social media profiles, or archived web pages. Such material remains subject to the general criminal-procedural requirements concerning examination, admissibility, and reliability (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 124–125). The framework, therefore, contains authentication mechanisms and general evidentiary standards, but not a uniform digital authentication procedure applicable to all forms of electronic information.

Third, there is a preservation gap. The Criminal Procedure Code already contains significant preservation mechanisms. Factual data may be fixed through procedural records; scientific and technical means must be documented when used during investigative actions; and information obtained through covert collection from computers or servers must be recorded on a material carrier, packaged, sealed, certified, and transferred (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 123, 199, 245). These provisions demonstrate that the protection of integrity already forms part of Kazakhstan's procedural framework. Nevertheless, no single statutory regime applies uniformly to all digital evidence and expressly requires measures such as forensic copying, cryptographic hash verification, preservation of relevant metadata, or a continuous documented digital chain of custody. Such safeguards are recognised in digital-evidence preservation and forensic guidance as important mechanisms for protecting integrity and traceability (Guttman et al., 2022; Kent et al., 2006). The gap is therefore one of uniform procedural coverage, not total legislative absence.

Fourth, there is a cross-border procedural gap. Kazakhstan law provides a legal mechanism for international legal assistance and expressly extends it to trafficking-related criminal cases (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Section 12; Law on Countering Human Trafficking, 2024, Art. 12(3)). What remains insufficiently specific is the treatment of digital information whose availability, integrity, or evidentiary context may deteriorate during formal international cooperation. Server location, platform retention policies, divergent disclosure procedures, different authentication practices, and variations in certification requirements may interrupt the continuity between foreign-held source data and the information ultimately presented in Kazakhstan. A mechanism for legal cooperation therefore exists, but a harmonised technology-specific framework for rapid preservation and cross-border authentication remains underdeveloped.

Taken together, these findings indicate that the central deficiency is not the absence of digital information from Kazakhstan's evidentiary framework nor the complete absence of rules regulating its use. The more precise problem is the absence of a sufficiently coherent, technology-specific procedural route by which heterogeneous forms of digital information can be consistently authenticated, preserved, attributed, and transformed into reliable evidence for judicial use. The Criminal Procedure Code establishes general requirements concerning lawful acquisition, fixation, examination, admissibility, reliability, and evidentiary evaluation; the Digital Code provides important concepts and authentication mechanisms for the digital environment; and the Law on Countering Human Trafficking supplies a framework for international cooperation (Criminal Procedure Code of the Republic of Kazakhstan, 2014; Digital Code of the Republic of Kazakhstan, 2026; Law on Countering Human Trafficking, 2024). What remains fragmented is the procedural interface among these legal regimes.

This normative gap supports the development of a hybrid evidentiary model for human trafficking proceedings. Such a model would not replace the existing evidentiary categories. Rather, it would connect them through clearer procedural safeguards adapted to digital material. Operational-investigative activity may identify relevant digital sources; criminal-procedural actions provide the legal mechanism for

acquiring and fixing those sources; digital-forensic safeguards can support authenticity, integrity, provenance, and attribution; and the resulting factual data remain subject to the general judicial standards of relevance, admissibility, reliability, and sufficiency. The contribution of this model is therefore procedural rather than technological: it demonstrates how established criminal-procedure requirements can be operationalised when the underlying source of proof is digital, reproducible, technically mutable, and potentially transnational.

DISCUSSION

The findings of this study reveal three interrelated dimensions of the evidentiary problem in human trafficking proceedings in Kazakhstan. First, the circumstances that must be proved are offence-specific and cannot be reduced to a single universal formula applicable to every form of trafficking. The statutory requirements differ according to whether the prosecution concerns the purchase or sale of a person, another transaction concerning a person, or acts such as recruitment, transportation, transfer, harbouring, and receipt for the purpose of exploitation (Penal Code of the Republic of Kazakhstan, 2014, Art. 128; Supreme Court of the Republic of Kazakhstan, 2012, para. 2). Second, information acquired during an investigation does not derive its evidentiary value solely from its factual relevance. Operational-investigative information must enter criminal proceedings through legally recognised mechanisms and remain subject to rules governing collection, fixation, examination, admissibility, reliability, and sufficiency (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 111–125; Law on Operational Investigations, 1994, Art. 14). Third, Kazakhstan already recognises various forms of computer and digital information, but the procedural safeguards applicable to their authentication, preservation, attribution, integrity, and cross-border acquisition remain fragmented across criminal-procedure, operational-investigative, and digital legislation (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 118–120, 231–245; Digital Code of the Republic of Kazakhstan, 2026, Arts. 49–50, 62–64). Taken together, these findings demonstrate that the central evidentiary challenge is not simply obtaining information about trafficking, but converting heterogeneous sources of information into legally reliable evidence capable of supporting judicial findings.

The first finding is significant because it shows why trafficking prosecutions require a differentiated evidentiary strategy. The legal structure of the offence determines the structure of proof. Purchase, sale, recruitment, transportation, harbouring, exploitation, and other conduct cannot be treated as evidence-interchangeable because different statutory forms may require proof of distinct objective and subjective circumstances. In particular, exploitative purpose is a mandatory element for recruitment, transportation, transfer, harbouring, receipt, and comparable acts directed toward exploitation, whereas the purchase, sale, or another transaction concerning a person is not subject to the same purpose requirement (Supreme Court of the Republic of Kazakhstan, 2012, para. 2). This finding supports the broader observation of Fouladvand and Ward (2023) that legal categories of human trafficking shape the way conduct is identified, classified, and prosecuted. The present study develops that insight at the evidentiary level: legal categorisation does not merely determine the name of the offence but also determines which facts must be established and what forms of evidence are needed to establish them.

This differentiated structure also explains why reliance on a single source of evidence is particularly problematic in trafficking proceedings. Victim testimony may be indispensable for reconstructing recruitment, control, exploitation, dependence, or coercive circumstances, but the evidentiary architecture of the offence frequently requires corroboration through communications, financial records, travel information, documentary materials, medical or psychological assessments, and other factual data. Nichols

and Heil (2024) emphasise that survivors may be reluctant to participate in conventional prosecutions for a range of reasons and therefore advocate a more survivor-centred and integrated prosecution framework. Hounmenou and Toepp (2023) similarly identify victim-centred practice, inter-agency collaboration, and the limitations of exclusively criminal-enforcement approaches as important concerns in trafficking investigations. The present findings complement these studies by demonstrating why reduced dependence on a single testimonial source is also important as a matter of evidentiary design. A multi-source evidentiary structure can strengthen the evidence of legally relevant circumstances while reducing the risk that the entire prosecution depends on the continued availability, willingness, or capacity of an individual victim to testify.

The second finding clarifies a distinction that is often obscured when investigation and proof are discussed as though they were the same process. Kazakhstan law permits materials obtained through operational-investigative activity to contribute to criminal proof, but their evidentiary use depends upon verification and incorporation in accordance with criminal-procedure requirements (Law on Operational Investigations, 1994, Art. 14; Criminal Procedure Code of the Republic of Kazakhstan, 2014, Art. 120). Covert investigative actions follow an even more specific procedural route, involving statutory authorisation, transmission, examination, fixation, and evaluation before their results can be relied upon to prove a criminal case (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 231–239). The significance of this finding is that factual usefulness and evidentiary validity are analytically distinct. Information may correctly identify a trafficker, victim, communication channel, payment, or location, but still fail to perform a judicial evidentiary function if its acquisition or incorporation does not satisfy mandatory procedural requirements.

This distinction extends earlier research on the practical investigation and prosecution of trafficking. Ward and Fouladvand (2021), for example, demonstrate the potentially important role of expert evidence while also emphasising the need to scrutinise its reliability. Bjelland (2020) shows that success in policing human trafficking cannot be understood exclusively through conventional measures such as convictions and sentencing outcomes because trafficking investigations involve competing organisational and victim-related considerations. The present study adds a procedural dimension to these observations. Investigative success should not be equated automatically with evidentiary success. Locating a victim, identifying a trafficking network, obtaining a communication, or acquiring an expert interpretation represents an investigative achievement; whether that information can support prosecution depends on its lawful transformation into one of the evidentiary forms recognised by criminal procedure. The concept of procedural transformation, therefore, shifts the analysis from the quantity of information collected to the legal quality of the evidentiary process through which that information becomes capable of judicial use.

The third finding becomes particularly important as trafficking activity increasingly generates online and computer-derived traces. De Vries and Radford (2022) demonstrate that online environments can contain observable markers of trafficking and other difficult-to-observe criminal activities. Their work establishes the analytical value of online traces for detection. The present study extends that line of inquiry from detection to admissibility. Discovering relevant online content does not, by itself, resolve the evidentiary questions raised by screenshots, social media messages, metadata, archived webpages, account information, or server records. Kazakhstan's Criminal Procedure Code already allows computer information, photographs, sound recordings, video recordings, and other technically recorded material to be admitted into criminal proceedings through existing evidentiary categories (Criminal Procedure Code of the Republic of Kazakhstan, 2014, Arts. 118–120). The Digital Code further establishes concepts and

integrity mechanisms relating to electronic documents, digital documents, digital data, and electronic digital signatures (Digital Code of the Republic of Kazakhstan, 2026, Arts. 49–50, 62–64). The gap identified by this study is therefore not one of complete legal non-recognition. It is the absence of sufficiently uniform procedures for addressing authenticity, provenance, attribution, integrity, preservation, and reproducibility across heterogeneous forms of digital evidence.

This distinction between legal recognition and procedural specificity is particularly consequential in transnational trafficking cases. Dandurand and Jahn (2020) question the effectiveness of the international legal architecture governing trafficking and migrant smuggling, while Dandurand (2024) argues that persistent failures in trafficking enforcement are linked not only to legal frameworks but also to deficiencies in proactive investigation and international law enforcement cooperation. The findings of the present study refine this problem in relation to digital evidence. Kazakhstan provides legal mechanisms for international assistance in trafficking-related criminal cases, including cooperation under applicable treaties or, in their absence, reciprocity procedures established by criminal-procedure law (Law on Countering Human Trafficking, 2024, Art. 12(3)). The difficulty is that conventional international legal-assistance mechanisms operate on digital information that may be altered, deleted, or relocated, or be subject to limited provider retention periods. Thus, the existence of a legal mechanism for international cooperation does not necessarily guarantee the timely preservation or technical continuity of the evidence ultimately received. This tension between formal cooperation and the temporal characteristics of digital data represents an important procedural dimension of contemporary transnational trafficking enforcement.

The theoretical contribution of these findings is the proposed hybrid evidentiary model. The model does not require digital evidence to replace conventional evidence or necessarily to become an autonomous statutory category. Instead, it conceptualises trafficking proof as an interconnected sequence. Operational-investigative activity identifies potentially relevant persons, locations, communications, transactions, and digital sources; criminal-procedural actions provide the legal route for acquiring, verifying, and fixing relevant factual information; digital-forensic safeguards support authenticity, integrity, provenance, and attribution where the source is electronically stored or transmitted; and the resulting material remains subject to judicial standards of relevance, admissibility, reliability, and collective sufficiency. In this sense, the model's contribution is procedural rather than technological. It explains how different information environments can be connected through a common evidentiary architecture without collapsing the distinction between intelligence, investigation, and judicial evidence.

This model also provides a broader interpretation of the relationship between information and proof. Digitalisation has increased the volume and diversity of traces potentially available to investigators, but information abundance does not necessarily produce evidentiary sufficiency. The more consequential issue is whether the origin, continuity, authenticity, and meaning of those traces can be demonstrated through procedures that are subject to judicial verification. This interpretation is consistent with Ward and Fouladvand's (2021) emphasis on critical scrutiny of expert evidence and with digital-evidence preservation guidance that stresses source documentation, integrity verification, and continuity of handling (Guttman et al., 2022; Kent et al., 2006). The same principle applies beyond technical evidence: the legitimacy of trafficking prosecutions depends not only on obtaining incriminating information but also on ensuring that the process by which that information becomes evidence is transparent, verifiable, and compatible with procedural rights.

The hybrid model nevertheless involves an important tension. Strong procedural safeguards serve positive functions: they protect evidentiary reliability, facilitate judicial scrutiny, support the rights of the

accused, and reduce the possibility that manipulated, incomplete, or incorrectly attributed digital material will influence criminal adjudication. At the same time, procedural requirements may become dysfunctional if they are too fragmented, slow, or poorly adapted to volatile electronic data. An online advertisement may disappear, an account may be deleted, server records may expire, or remotely stored material may change while formal procedural authorisation or international assistance is being pursued. The appropriate policy response is therefore not to weaken admissibility safeguards, but to make them sufficiently clear, technically informed, and operationally efficient. This is particularly important in trafficking cases, where victim protection and evidentiary preservation may both depend on timely investigative intervention.

The findings consequently generate several implications for legal and institutional reform. First, Kazakhstan should develop authoritative procedural guidance specifically addressing the acquisition, authentication, preservation, attribution, and presentation of major categories of digital evidence, while maintaining the existing evidentiary standards of the Criminal Procedure Code. Second, such guidance should distinguish current statutory requirements from technical safeguards appropriate to screenshots, metadata, messaging data, archived webpages, digital devices, and provider-held information. Recommended measures may include documentation of the source and acquisition process, preservation of relevant metadata, forensic copying where appropriate, cryptographic integrity verification, and a documented chain of custody, consistent with established digital-forensic guidance (Guttman et al., 2022; Kent et al., 2006). Third, procedures under the Criminal Procedure Code, the Digital Code, and trafficking legislation should be aligned so that investigators, prosecutors, specialists, and courts operate with a coherent understanding of digital material. Fourth, institutional capacity should be strengthened through specialised training and access to competent digital-forensic expertise. Fifth, cross-border cases require mechanisms capable of rapidly preserving provider-held data before or alongside formal mutual legal-assistance procedures, while ensuring that subsequent acquisition and transfer comply with applicable law. These measures would operationalise rather than replace the general requirements of legality, admissibility, reliability, and verification that already govern Kazakhstan's evidentiary system.

Overall, the discussion demonstrates that the effectiveness of human trafficking prosecution depends on the relationship among substantive offence structure, investigative information, procedural transformation, and digital evidentiary integrity. Previous scholarship has separately identified the difficulties of trafficking policing, victim participation, expert evidence, online detection, inter-agency collaboration, and international enforcement (Bjelland, 2020; de Vries & Radford, 2022; Dandurand, 2024; Hounmenou & Toepp, 2023; Nichols & Heil, 2024; Ward & Fouladvand, 2021). The present study connects these concerns through a normative evidentiary framework. Its principal contribution is therefore to show that the contemporary challenge of proving trafficking is not resolved simply by collecting more information or deploying more advanced technology. Effective prosecution requires a legally coherent pathway through which offence-specific facts, operational information, conventional evidence, and digital traces can be transformed into reliable and admissible proof while preserving both procedural legitimacy and the capacity to respond effectively to the transnational and technologically mediated character of trafficking.

CONCLUSION

This study demonstrates that the central challenge in proving human trafficking in Kazakhstan lies not merely in collecting relevant information, but in ensuring that such information is transformed into

evidence through legally recognised and reliable procedural mechanisms. Three principal findings emerge. First, the normative structure of proof in human trafficking cases is offence-specific and multi-layered; different forms of conduct under Kazakhstan's criminal law require proof of different objective, subjective, victim-related, and aggravating circumstances. Second, operational-investigative information does not automatically acquire the same legal status as evidence admissible in judicial proceedings. Its evidentiary value depends on lawful collection, verification, procedural fixation, incorporation into a recognised evidentiary form, and subsequent assessment of relevance, admissibility, reliability, and sufficiency. Third, Kazakhstan already provides legal recognition for various forms of computer and digital information, but the applicable rules remain fragmented and insufficiently specific regarding authentication, attribution, integrity, preservation, the digital chain of custody, and cross-border electronic evidence. The principal regulatory problem is therefore not the absence of digital evidence in the legal framework, but the absence of a sufficiently coherent procedural pathway to transform heterogeneous digital information into reliable judicial proof.

The main scientific contribution of this study is the development of the concept of procedural transformation and its integration into a hybrid evidentiary model for human trafficking proceedings. The model connects three previously fragmented dimensions of proof: the substantive circumstances that must be established in law, the procedural mechanisms by which investigative information acquires evidentiary status, and the additional safeguards required when the underlying information is digital. This approach moves beyond a descriptive classification of investigative techniques by explaining how operational information, conventional evidence, and digital traces can be integrated within a single evidentiary architecture. The study also contributes a clear distinction between *lex lata* and *lex ferenda* in the treatment of digital evidence. Practices such as forensic copying, hash verification, metadata preservation, a documented chain of custody, and structured web content preservation are therefore identified as recommended safeguards for strengthening authenticity and integrity, rather than being incorrectly presented as universally applicable requirements of current Kazakhstan law. This distinction provides a more precise doctrinal basis for the future development of criminal procedural rules governing digital evidence.

The study is nevertheless limited by its normative and doctrinal design. Its findings are derived primarily from legislation, Supreme Court normative interpretations, international legal instruments, and relevant technical guidance and therefore do not establish how these rules are consistently applied in individual trafficking investigations or judicial proceedings. The study did not examine criminal case files, judgments in a systematic empirical sample, prosecutorial practices, interviews with investigators and digital-forensic specialists, or the practical operation of cross-border requests for platform-held data. Consequently, the proposed hybrid evidentiary model should be tested in future empirical and comparative research. Further studies could examine trafficking case files and judicial decisions to determine how digital evidence is actually authenticated and challenged, investigate the practices of law enforcement and forensic institutions, and compare Kazakhstan's procedural framework with jurisdictions that have developed more specific rules for electronic evidence. Such research would help determine how the doctrinal model proposed in this study can be translated into effective procedural standards and institutional practice.

REFERENCES

- Bjelland, H. F. (2020). Conceptions of success: Understandings of successful policing of human trafficking. *Policing: A Journal of Policy and Practice*, 14(3), 712–725. <https://doi.org/10.1093/police/pay073>
- Dandurand, Y. (2024). Criminalizing human trafficking has not made a difference: A law enforcement failure. *Journal of Human Trafficking*, 10(2), 383–387. <https://doi.org/10.1080/23322705.2024.2303266>
- Dandurand, Y., & Jahn, J. (2020). The failing international legal framework on migrant smuggling and human trafficking. In J. Winterdyk & J. Jones (Eds.), *The Palgrave international handbook of human trafficking* (pp. 783–800). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-63058-8_47
- de Vries, I., & Radford, J. (2022). Identifying online risk markers of hard-to-observe crimes through semi-inductive triangulation: The case of human trafficking in the United States. *The British Journal of Criminology*, 62(3), 639–658. <https://doi.org/10.1093/bjc/azab077>
- Fouladvand, S., & Ward, T. (2023). Criminal law categories as ideological constructs: The case of human trafficking. In D. G. Scott & J. Sim (Eds.), *Demystifying power, crime and social harm: The work and legacy of Steven Box* (pp. 299–324). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-46213-9_12
- Guttman, B., White, D. R., Williams, S., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers* (NISTIR 8387). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8387>
- Hounmenou, C., & Toepp, S. (2023). Exploring private investigation agencies' experience of collaboration with law enforcement in investigations of human trafficking cases. *Societies*, 13(2), Article 44. <https://doi.org/10.3390/soc13020044>
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>
- Nastas, A. (2024). *Specifics of human trafficking crime investigation*. ADJURIS – International Academic Publisher.
- Nichols, A. J., & Heil, E. J. (2024). An integrated model of human trafficking response in the prosecution process: Restorative justice, therapeutic jurisprudence, survivor centered practice and anti-oppressive practice. *Crime, Law and Social Change*, 81(3), 231–253. <https://doi.org/10.1007/s10611-023-10114-w>
- Pajón, L., & Walsh, D. (2020). Proposing a theoretical framework for the criminal investigation of human trafficking crimes. *Policing: A Journal of Policy and Practice*, 14(2), 493–511. <https://doi.org/10.1093/police/pay031>
- United Nations Office on Drugs and Crime. (2020). *Global report on trafficking in persons 2020*. United Nations.
- United Nations Office on Drugs and Crime. (2021). *Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons* (CTOC/COP/WG.4/2021/2). United Nations.
- Ward, T., & Fouladvand, S. (2021). Bodies of knowledge and robes of expertise: Expert evidence about drugs, gangs and human trafficking. *Criminal Law Review*, 2021(6), 442–460.

Legislation, International Instruments, and Judicial Authorities

Criminal Procedure Code of the Republic of Kazakhstan, Code of the Republic of Kazakhstan No. 231-V ZRK (2014). Adilet Legal Information System. <https://adilet.zan.kz/eng/docs/K1400000231>

- Digital Code of the Republic of Kazakhstan*, Code of the Republic of Kazakhstan No. 255-VIII ZRK (2026). Adilet Legal Information System. <https://adilet.zan.kz/eng/docs/K2600000255>
- Law on Countering Human Trafficking*, Law of the Republic of Kazakhstan No. 110-VIII LRK (2024). Adilet Legal Information System. <https://adilet.zan.kz/eng/docs/Z2400000110>
- Law on Electronic Document and Electronic Digital Signature*, Law of the Republic of Kazakhstan No. 370 (2003) (repealed 2026). Adilet Legal Information System. https://adilet.zan.kz/eng/docs/Z0300000370_
- Law on Operational Investigations*, Law of the Republic of Kazakhstan No. 154-XIII (1994). Adilet Legal Information System. https://adilet.zan.kz/eng/docs/Z940004000_
- Penal Code of the Republic of Kazakhstan*, Code of the Republic of Kazakhstan No. 226-V (2014). Adilet Legal Information System. <https://adilet.zan.kz/eng/docs/K1400000226>
- Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime*, 2237 U.N.T.S. 319 (2000).
- Supreme Court of the Republic of Kazakhstan. (2012). *On practice for enforcement of the legislation establishing liability for human trafficking* (Normative Decree No. 7 of December 29, 2012; as amended through November 29, 2024). Adilet Legal Information System. <https://adilet.zan.kz/eng/docs/P120000007S>
- Supreme Court of the Republic of Kazakhstan. (2020). *On authorization of covert investigative actions* (Regulatory Resolution No. 5 of December 11, 2020). Adilet Legal Information System. <https://adilet.zan.kz/eng/docs/P200000005S>