PROTECCIÓN DE DATOS CONFIDENCIALES EN ASIA CENTRAL PARA GARANTIZAR DERECHOS HUMANOS Y SEGURIDAD PÚBLICA

CONFIDENTIAL DATA PROTECTION IN CENTRAL ASIA TO ENSURE HUMAN RIGHTS AND PUBLIC SECURITY

DOI: https://doi.org/10.17981/juridcuc.21.1.2025.12

Fecha de Recepción: 2025/07/14 Fecha de Aceptación: 2025/10/01

Nazgul Ibrayeva
Astana International University, Kazakhstan
nazgul.ibrayeva@mymail.academy

Mukhabbatkhon Agzamova
International Islamic Academy of the Republic of Uzbekistan, Uzbekistan
agzamova@mymail.academy

Ilyos Abdullayev
Urgench State University, Uzbekistan
abdullayev@mymail.academy

Elvir Akhmetshin
Mamun University, Uzbekistan
elvir@mymail.academy

Aleksandr Kiselev
Financial University under the Government of the Russian Federation, Russia
kiselev@mymail.academy

Para citar este articulo:
Ibrayeva, N., Agzamova, M., Abdullayev, I., Akhmetshin, E. y Kiselev, A. (2025). Protección de datos confidenciales en Asia central para garantizar derechos humanos y seguridad pública. *Jurídicas CUC, 21*(1), pp. 232 - 246. DOI: http://doi.org/10.17981/juridcuc.21.1.2025.12

Resumen
La protección de datos confidenciales en Asia Central cobra importancia en un momento en que la gobernanza digital. Si bien la investigación internacional suele destacar las experiencias europeas, Asia Central permanece poco explorada, lo que crea una novedad regional que este artículo busca abordar. El estudio aplicó un enfoque de análisis documental que revisa las leyes nacionales, la literatura académica y los instrumentos internacionales. Se analizaron los sistemas jurídicos de Asia Central en materia de datos personales confidenciales y se reflexionó sobre su compatibilidad con las normas internacionales y europeas, en particular la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH). La metodología se basa en los principios interpretativos desarrollados para la aplicación del artículo 8 del Convenio Europeo de Derechos Humanos. Estos principios enfatizan la legalidad y la proporcionalidad, y desarrollan salvaguardias al equilibrar la seguridad del Estado y la privacidad individual. La legislación de Asia Central carece de definiciones precisas de datos sensibles. Además, ofrece mecanismos débiles para la protección transfronteriza, así como una aplicación fragmentada. En contraste, la jurisprudencia del TEDH interpreta de forma coherente, incluso ofreciendo herramientas que protegen los derechos humanos, sin dejar de preocuparse legítimamente por la seguridad pública. Para que Asia Central pueda conciliar la seguridad pública con los derechos humanos, debe definir sus leyes de forma armoniosa, aclarar las condiciones de procesamiento de manera extraordinaria y adoptar fuertes salvaguardias técnicas y organizativas que estén en línea con los estándares internacionales.

Palabras clave: Protección de datos, Derechos humanos, Legislación, Seguridad pública, Sistemas jurídicos, Derecho internacional.

Abstract
Confidential data protection in Central Asia presses in a time when digital governance expands so rapidly and implies so many things for public security and human rights. Although international research often stresses European experiences, Central Asia remains underexplored, also this creates a regional novelty that this article seeks to address. A document analysis approach that reviews national laws, academic literature, also international instruments was applied in the study. Analysis of Central Asian legal systems regarding confidential personal data plus reflection on compatibility with international and European standards especially European Court of Human Rights (ECHR) jurisprudence occurred. Interpretive principles developed for applying Article 8 of the European Convention on Human Rights inform the methodology. These principles do stress legality and proportionality also they do evolve safeguards as they balance state security and individual privacy. Central Asian legislation lacks in precise definitions of sensitive data. Furthermore, it provides weak mechanisms for cross-border protection as well as fragmented enforcement. In contrast, ECHR jurisprudence coherently does interpret, even offering up tools that do protect human rights while still legitimately concerning public security. In order for Central Asia to reconcile public security with human rights, it must define its laws in a harmonious way, clarify processing conditions in an extraordinary way, and adopt strong technical and organizational safeguards that are aligning with international standards.

Keywords: Data protection, Human rights, Legislation, Public security, Legal systems, international law.

INTRODUCTION

One of the most important international legal acts safeguards as well as surrenders personal data then is the Council of Europe Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data (hereinafter referred to as the Convention) (Council of Europe, 1981), which all countries that have ratified it find binding. Personal data is subject to a definition per Article 2 of the Convention. This constitutes details pertaining to a particular or discernible individual, otherwise regarded as a data subject (Rupp & von Grafenstein, 2024). This formulation appears in almost the same form in all the internal legislative acts of the participating countries, which is reflected in the Federal Law of the Russian Federation "On Personal Data" (hereinafter referred to as the Law) (Russian Federation, 2006).

The Law identifies an exhaustive list of conditions under which authorized persons may process a subject's personal data. Only in these cases will the data processing be legitimate; otherwise, it will be considered illegal. According to the Law, since it determines the content for basic definitional concepts, someone processes personal data when that individual executes any action or collection of actions, like collection, recording, systematization, amassing, storage, clarification (updating, modification), extraction, usage, transferral (distribution, provision, access), depersonalization, blocking, deletion, also destruction, inclusive of through using information (automated) systems (Article 3). In the Russian legal field, all these actions are considered types of processing private information about an individual (Vasyukov, 2021).

International legislation has developed the relevant legal tools in detail, coupled with the European Court of Human Rights effectively enforcing law via those tools to implement each of these procedures for processing personal information (Novelli et al., 2024). The method for conveying data to other individuals, for instance when data are conveyed across state lines, is especially precisely governed (Bossi, 2021). Global regulations postulate that data dispersal concerns one person's personal existence. Disclosing it to other individuals absent the subject's assent is permissible solely if established by law (Marelli, 2024).

Processing data about one's personal life should be carried out to exclude the possibility of unauthorized access or use and loss or destruction of information (Semenov & Lysenko, 2021; Khoulimi & Benammar, 2024). In a significant number of cases where personal data relates to fundamental aspects of human life, after using them to achieve an appropriate legitimate goal, they must be destroyed by the owner and in no case used for other purposes contrary to the interests of the individual (Lachina et al., 2021). Today, personal data is information in an electronically oriented or catalog form containing information about an individual's private life that can be identified based on this information (Esmail et al., 2024; Petrov et al., 2024).

Multiple studies analyze various aspects of personal data processing and protection (Dmitrieva, 2021), the international experience of legal regulation of these relations (Danelian et al., 2023; T-Trang Lâm, 2024), the implementation of the state information policy (Uvizheva et al., 2020; Mahdy et al., 2025), and international information policy (Kohler, 2016; Neznamova et al., 2020). However, doctrinal research has not yet

paid enough attention to the specificity of the processing of individual personal data, particularly in the context of their increased importance for ensuring the inseparable human right to confidentiality.

Therefore, the paper aims to study the current legislation regulating legal instruments for processing and transmitting certain types of personal information and analyze existing law enforcement practices. Necessary steps will be proposed to advance society towards fair protection of the most vulnerable human data.

The primary method used in the study was document analysis. It was based on different types of materials depending on the focus of our research. First, a group of materials (research articles, monographs, conference abstracts) revealed the theoretical and legal aspects of protecting confidential categories of personal data.

The second block of materials consisted of international legislative acts (Council of Europe, 1981; 1987; European Parliament & Council of the European Union, 1995; 2016). And the third block consisted of materials from the ECHR's judicial practice regarding applying Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (European Court of Human Rights, 1997; 2002; 2003; 2007; 2008; 2015; 2020).

International organizations that promulgate and administer data protection instruments construe systems uniquely to guarantee uniform implementation across jurisdictions. The Council of Europe with the European Court of Human Rights construe teleologically plus evolutively, understanding Convention articles regarding current conditions also highlighting proportionality when nations constrain privacy entitlements (European Court of Human Rights, 1997; 2008).

Likewise, the European Union employs an organized exegesis in the GDPR since it incorporates human dignity and basic rights into each prescriptive stipulation (European Parliament & Council of the European Union, 2016; Kohler, 2016). United Nations entities embrace teleological elucidation. They contextualize data confidentiality inside the wide-ranging entitlement to privacy under Article 17 of the ICCPR (United Nations Human Rights Committee, 2014) via soft law instruments such as General Assembly resolutions and Human Rights Committee general comments. As they mold the phrasing and realistic application of lawful principles scrutinized in this writing, accentuating those customs is vital.

Current protection mechanisms for confidential data operate on two complementary levels. Unequivocal consent stipulations, strict terms upon special data processing, surveillance's judicial monitoring, together with data subject entitlements such as access, rectification, plus erasure represent legal protections (Council of Europe, 1981; European Parliament & Council of the European Union, 1995; 2016). Technical as well as organizational safeguards anonymize, encrypt, store in a secure manner, control access, and further empower independent supervisory authorities so they may monitor compliance then impose sanctions (Feng et al., 2024; Gasiokwu et al., 2025).

Concurrently, these modalities endeavor to preclude impermissible access, assure that processing remains licit, and ascertain that the state functions commensurately during the invocation of public security justifications. These safeguards are elucidated to highlight the disparity within Central Asian legislation and the more fortified

European frameworks. Some of the Central Asian instruments are not well developed yet, so European systems utilize them to implement human rights protections (Petrov et al., 2024; Neznamova et al., 2020).

DISCUSSION

Theoretical and legal aspects of protection of confidential categories of personal data

According to researchers, the law of many countries has long established with applied the axiom that when individuals handle private personal data, like information concerning health, suspicion regarding commission of a crime, the existence of charges, or the employment of procedures, together with actions, for assessment of one's abilities or conduct or for restriction of their entitlements, inclusive of instances where individuals undertake it under some agreement, it constitutes a distinct menace for individual entitlements as well as liberties (Alkhariji et al., 2023; Golightly et al., 2023; Petrov et al., 2024). In national legislation on personal data protection, the privacy criterion is used to classify personal information into data categories that are generally prohibited from processing or need to be processed with increased protection measures (Navarro-Hernández, et al., 2022; Feng et al., 2024). The internal law either directly indicates the assignment of a specific group of data to a particular category or gives authorities (usually the minister in charge of the national data protection agency, sometimes the prime minister) the authority to make operational decisions on this issue.

The list of personal data that is considered confidential and requires special careful protection in terms of their collection, processing, and dissemination is determined by national traditions, mentality, cultural and religious customs, etc. (Danelian et al., 2023; Lorincz, 2023). Therefore, it may vary from society to society (Kurnianti et al., 2024; Abikenov et al., 2025). General rules of legal orientation, defined by convention principles and including vulnerable data on racial and ethnic origin, religious identity, political preferences, participation in professional and social organizations, criminal history, health status, and sexual behavior, are in force in all countries (Anbari et al., 2022).

Since the current regulations, both national and international, cannot establish in detail an exclusive list of the most vulnerable blocks of information about an individual's personal life (especially since, in specific situations, the same information for individual subjects may be confidential or not (Fernandez-Costales Muñiz 2024; Alazzam et al., 2025), the scientific literature has developed specific visions on this issue. Thus, at the general theoretical level, it is customary to use confidential personal data to indicate information about arrests, credit histories, and reports, work activities in terms of assessing an employee's professional abilities and business qualities, banking information, and medical and tax data (European Parliament & Council of the European Union, 1995).

The most successful criterion for the confidentiality of personal data is formulated in (Søe et al., 2021; Keesal et al., 2025), according to which personal information could be defined as those facts, messages, or opinions related to a given person and regarding

which it would be expected that the subject considers them intimate or confidential, and accordingly, would like to stop or at least limit their circulation.

Based on the criteria of sensitivity of personal information, some researchers divide it into nominative and other information (Dmitrieva, 2021; Danelian et al., 2023). Here, the information identifying a specific person (surname, first name, patronymic, gender, passport series and number, date and place of birth, etc.) is postulated as nominative (Krishnan et al., 2025). Among the nominative data, a special place belongs to vulnerable information about biometric personal data, that is, information characterizing the physiological and biological characteristics of a person, based on which their identity can be established (Dmitrieva, 2021; Beig et al., 2024; Gasiokwu et al., 2025). Non-nominative data includes personal information with an additional, optional character and may also be classified as confidential, depending on the circumstances and the subject's perception of its importance. This includes information about income, place of work, political views, medical conditions, criminal records, etc. (Danelian et al., 2023).

In some practical situations, the classification of personal information as confidential depends on a particular person's subjective perception of it as confidential and their awareness of a possible violation of the right to confidentiality due to the processing and dissemination of this information. We consider this approach balanced and fair. Therefore, it should be considered when designing an appropriate regulatory mechanism, especially in judicial law enforcement.

Regulation of the protection of confidential categories of personal data in EU inter-state legal acts

For the first time, the Convention differentiated types of personal data based on their importance to the subject and the risks and threats to it in the event of the unlawful dissemination of the data (Article 6). This resulted in the concept of confidential personal data, the collection, processing, use, and transfer of which is prohibited altogether or requires special security and protection measures. In the absence of an outright prohibition, the processing of these categories of personal data is carried out in a special manner, separately regulated by law. The Convention established that personal data about race, political views, or religious and other beliefs cannot be subject to automated processing unless internal legislation establishes appropriate safeguards. That is, since processing such specific information can cause significant material and moral harm to the data subject, it is only possible in exceptional cases when the state introduces certain guarantees prescribed by law.

As a result of the European Parliament coupled with the Council of the EU adopting Directive 95/46/EC regarding the protection of individuals during processing personal data as well as freely moving such data in 1995, they identified special groups of so-called sensitive personal information from the thorough list of personal data. Their handling possesses meaningful subtleties. It is allowed solely in distinctly specified instances (European Parliament & Council of the European Union, 1995).

As the examination of these dictates revealed, private details concerning racial or ethnic heritage and political, religious, or philosophical convictions are part of the data

classification generally restricted from manipulation (Pop & Pop, 2023). A distinctive lawful framework sufficiently secures governmental oversight as it transmits private details also handles plus promulgates facts on partisan furthermore labor organization affiliation, penal verdicts, well-being, sexual existence, with biometric otherwise inherited particulars.

The Regulation of the European Parliament as well as of the Council superseded Directive 95/46/EC. The regulation of April 27, 2016, concerning personal data protection plus data movement also mirrored this position (European Parliament & Council of the European Union, 2016).

The political plus hermeneutical progression concerning European data protection norms remains misunderstood absent a reference to the Charter of Fundamental Rights of the European Union, proclaimed in Nice in December 2000 plus legally bound by the Treaty of Lisbon in 2009. In contrast to the European Convention on Human Rights, protecting privacy via Article 8 when it delineates the overarching entitlement to respect regarding private existence, the Charter safeguards data as a separate, foundational entitlement in Article 8. This differentiation represents the shift from privacy as a general human entitlement to data safeguard as a discrete assurance (European Parliament, Council & Commission, 2000). Regarding politics, the Charter augmented data protection toward the same normative stratum as dignity, freedom, and equality for it established a basis to ensuing implements like the GDPR (European Parliament & Council of the European Union, 2016; Kohler, 2016).

The Charter also buttressed interpretive principles that apprise the implementation of revised legislation: the principle of legality, which requires a clear legal basis for any interference with data; the principle of proportionality, which balances security objectives with minimal intrusion; along with the principle of accountability, which obliges controllers and supervisory bodies to guarantee compliance. European institutions steadfastly utilize these tenets for diminishing ambiguities within enforcement. This application additionally steers the judicial assessment process (Bossi, 2021; Petrov et al., 2024; Neznamova et al., 2020).

This progression is evident in the numerous by-laws that regulate activity rules in various industries and that specify the general principles of confidential data processing in the EU. An important act regulating the specifics of the relationship between participants in personal data dissemination is the Recommendation of the Committee of Ministers of the EU No. R(91) 10 on the communication to third parties of personal data held by public bodies (hereinafter referred to as the Recommendation) (Council of Europe, 1991). This act is based on the principle of respect for privacy and data protection.

Such a category of guarantees surfaced within the Recommendation for the first time because third parties communicate, notably by electronic means, personal data or files containing personal data; they should guarantee that they will not unlawfully violate the privacy of the data subject. Outside entities ought not to have private data along with files holding such disclosed to those entities. An allowance might exist under specific conditions, except in cases where:

1) this is provided by special law;

2) the public has access to them under the legal provisions governing access to public sector information;

3) notification is carried out following national legislation on information protection;

4) the data subject has freely and informatively given their consent.

Unless national law provides adequate safeguards for the data subject, personal data or files containing personal data may not be disclosed to third parties for purposes other than those for which the data was collected (Recommendation: clause 2). Special attention is paid to reservations that must be considered when distributing confidential data. These data should not be stored in a file or part of a file publicly available to third parties. Any exceptions to this principle should be provided by law, ensuring appropriate guarantees to the data subject (clause 3).

Separate Recommendations of the EU Committee of Ministers focus on regulating relations between collecting and processing personal data in special situations, such as during law enforcement activities. For example, we can mention Recommendation No. R(87) 15 of the Committee of Ministers to the Member States regulating the use of personal data in the police sector (Council of Europe, 1987) (approved on September 17, 1987, at the 410th meeting of Deputy Ministers). According to this act, the collection of personal data for police purposes should be limited to the extent necessary to prevent a real danger or to terminate a criminal offense of a special nature. Any exception to this provision should be subject to specific national legislation. Data collection by technical or other automated means can only be carried out following legal provisions. Gathering data about individuals must be barred solely because they possess specific racial heritages, religious faiths, sexual conduct, or political perspectives or are affiliated with movements or organizations without legal proscription, however. Principle 2 articulates that data relating to these matters may be amassed for a particular inquiry.

Law enforcement practice for the protection of confidential categories of personal data

Law enforcement practice plays a vital role in the legal mediation of confidential personal data turnover. International law enforcement decisions, particularly those issued by the ECHR regarding the application of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950, must be considered.

Our analysis of the ECHR's judicial practice showed that in decisions on specific cases, the ECHR indicates that concepts such as gender identification, name, sexual orientation, and sex life fall within the scope protected by Article 8. Information about a person's health status and ethnic origin is a particularly vulnerable element of private life.

The S and Marper v. the United Kingdom case (European Court of Human Rights, 2008) became a high-profile case, during which the ECHR used the rule of the national law, the UK Personal Data Protection Act [Data Protection Act] (adopted on July 16, 1998) (European Parliament & Council of the European Union, 1995) regarding the fact that vulnerable personal data includes personal information, including, among other things, information about race or nationality and the commission (probable commission) of a crime, the proceedings opened on the fact of a crime committed (probably committed), or

the punishment imposed by the court for this crime (Article 2). The ECHR was guided by the provisions of the report of the Nuffield Council on Bioethics of 2007 (Nuffield Council on Bioethics, 2007).

This enabled the ECHR to conclude that, given the possible further use of, among other things, cell samples, their systematic storage strongly affects human interests and may entail state interference in the exercise of the right to respect for private life. Therefore, the ECHR considers human concerns about the possible further use of stored private information legitimate and believes they should be considered when deciding whether state interference exists in implementing convention rights. Considering the rapid pace of genetics and information technology development, the ECHR cannot exclude the possibility that in the future, the state will be able to interfere in private life by using genetic information in new ways or in ways that cannot be accurately predicted today (cl. 70, 71). Therefore, the ECHR deduced that the state meddles with the applicants' rights for regard to their privacy when it keeps cell samples as well as DNA profiles in accordance with the provisions of part 1 of Article 8.

The Z v. Finland case (European Court of Human Rights, 1997) is significant for maintaining a balance of public and personal interests in protecting confidential data. In this case, during the criminal proceedings against the applicant's ex-husband, X, who had knowingly infected others with HIV, the courts authorized obtaining testimony from the applicant's doctor and psychiatrist regarding her medical condition, despite her disagreement. The courts authorized the seizure of the applicant's medical records without her consent and attached them to the criminal case materials against X. The local court ruled that the full text of the decision, which mentioned the applicant's last name, and the case documents would remain confidential for 10 years.

The Court of Appeal issued the full text of the decision, a copy of which was made available to the media, which mentioned the applicant's last name and her HIV status. The applicant complained about these facts to the ECHR under Article 8. She also stated that, contrary to Article 13 of the Convention, she had not been provided with effective judicial remedies for her complaints under Article 8. In her appeal, Z complained, among other things, about the failure of the Finnish State authorities to prevent the press from disclosing her identity and medical status as a carrier of HIV.

The ECHR determined Article 8 was not contravened concerning mandates compelling the applicant's medical advisors to offer testimony or the appropriation of medical documents and their incorporation in the investigatory compendium. The ECHR considered that 3) the provision of public access to these materials since 2002, if this had been done, would have been grounds for a violation of Article 8 and 4) as a result, Article 8 on the publication of information about the applicant's identity and her state of health in the Court of Appeal decision would have been violated.

A similar case, R.T. v. Moldova (2020) (European Court of Human Rights, 2020), concerned the disclosure of the applicant's HIV-positive status in a certificate of release from military service. Under Article 8, the applicant complained that he had to show this certificate when updating his identity documents and in other situations, such as when applying for a new job.

However, in this case, the ECHR ruled that there had been a violation of Article 8, finding that the disclosure of HIV status in the certificate of release from military service violated the applicant's right to confidentiality of medical data since the Moldovan Government had not indicated which "legitimate purpose" of Article 8 was pursued in disclosing the applicant's illness. Moreover, the Government did not explain why it was necessary to include sensitive information about the applicant in the certificate, which may be required in many situations where his medical condition was not supposed to have any bearing. Consequently, such serious interference with the applicant's rights was found to be disproportionate and to violate Article 8.

In the Peck v. the United Kingdom case (European Court of Human Rights, 2003), with regard to Article 8, the claimant made an appeal against the circumstance that the video record from the closed-circuit television showing the applicant's suicide endeavor was furnished to the media, also consequently the picture bearing his likeness got published many times in the newspapers as well as the digital recording itself got openly broadcasted on TV.

The ECHR pointed out that the recording of the incident provoked more serious consequences than could be expected from such a situation. Thus, the publication of this video material significantly interfered with the applicant's right to respect for his private life. The ECHR drew attention to the fact that the City Council had not received the applicant's consent to show the video and had not received guarantees from the press regarding the concealment of the applicant's image in the relevant photos. The ECHR also did not identify proper or sufficient reasons for the city council's direct publication of the video material in the program "News about video surveillance systems".

The ECHR further noted that the facts of the applicant's voluntary appearance in the media, which subsequently took place, did not reduce the severity of the interference in his private life, nor did they serve as grounds for exempting the relevant institutions from the obligation to take care of the consequences of their previous actions against the applicant (i.e., the release of video material), as a result of which the applicant became a victim of serious interference with his right to respect for his private life as a result of the actions of local and national media.

The ECHR concluded that the facts of the transfer by the city council of the said video material to television and newspapers were not accompanied by the adoption of appropriate measures to safeguard the interests of the applicant and constituted a disproportionate and unfair interference with the applicant's right to respect for his private life, which was a violation of Article 8.

In the Toma v. Romania case (European Court of Human Rights, 2002), the ECHR also ruled that photographing the applicant during his pre-trial detention and transmitting these photographs and photographs of his criminal case to the press violated Article 8.

Article 8 also protects against the storage and use of false information. Criminal charges were brought against the applicant in the circumstances of the Semalettin v. Turkey case. During the proceedings, the police sent a notice to the court stating that the applicant already had two convictions for involvement in terrorist organizations. The applicant had indeed been tried twice for participation in terrorist organizations, but on both occasions, he had been acquitted. The applicant claimed that storing and

disseminating false information about his criminal past violated his rights under Article 8.

The ECHR ruled that the information the police had was related to his private life, as it had been systematically preserved and used. It related to events in the applicant's life that had already occurred long before. The ECHR concluded that such interference was unlawful since the police had failed to fulfill their duty to renew such information and enter information that the court had acquitted the applicant. However, there were legal grounds for his case in the criminal archives.

In the R.E. v. Great Britain case (European Court of Human Rights, 2015), the ECHR decided that individuals who oversee legal consultations in a police station may intercept phone calls connecting lawyers to clients. Even though Article 8 defended the privacy for all letters among people, the ECHR knew that it gave greater safeguards to data shared by attorneys plus their patrons because attorneys could not guarantee those letters stayed private. Consequently, the ECHR regarded that overseeing legal discussions encroached to a supremely elevated extent upon one's entitlement to venerate their personal existence and communications. Individuals examining these documents presume equivalent protections are implemented. These protections are requisite for instances including communications interception; they shall shield persons against unwarranted infringement upon their rights per Article 8, undeniably as these tenets pertain toward this surveillance type.

CONCLUSIONS

Study has revealed that national legislation in several Central Asian along with European countries fails to safeguard confidential personal data since it stays disjointed, uncertain, but also frequently diverges from international standards. For effective implementation, national legal systems often require precision, enforceability, and consistency. In contrast, the Council of Europe Convention and the jurisprudence of the European Court of Human Rights provide explicit guidelines and protections that national frameworks could emulate.

During our assessment of prevailing legal mechanisms, we unearthed an important deficiency. These mechanisms insufficiently categorize and govern confidential information, notably within transnational environments. Judicial precedents from the European Court of Human Rights further stress that proportionality, legality, with strong safeguards are urgently needed when states interfere with private data. Statutory changes stressing worldwide benchmark synchronization, greater clarity, and strong implementation structure evolution promote accordance among domestic with multinational infrastructures. It is important, in addition to legal actions, to institute structural and technological resolutions to avoid abuse and forbidden access to private information.

From a hermeneutical perspective, three categories can classify the shortcomings into. Initially, normative deficiencies arise because statutes ambiguously delineate sensitive data, and cross-border regulations exhibit a lack of potency. Subsequently, flawed interpretations weaken the proportionality principle via excessively wide-ranging

national security rationales. Third, rights violations weaken privacy and dignity, coupled with informational self-determination through insufficient guarantees. These inadequacies highlight the partial conceptual manner Central Asian systems obtain basic and civil rights. For surmounting such impediments, legislators as well as courts must embrace construing models coherent to international custom, notably those fashioned under Article 8 of the ECHR and Article 8 of the EU Charter of Fundamental Rights. This methodology should guarantee cohesion in addition to narrowing hermeneutic fissures. It would harmonize public safety requests alongside the need for protecting human rights.

Eventually, the results from this analysis aid in pinpointing optimal methods for governing the transmission of private individual records. Consistent legal policies anchored to human rights may be formulated with these perceptions. Regarding assorted jurisdictions, public safety may be improved by policies upholding privacy.

REFERENCES

Abikenov, Zh., Syzdykova, M., Abdiramanova, A., Kudaibergenov, S. (2025). The Role of Religious Spirituality in the Social Development of Public Consciousness: An Approach to Interpersonal Relationships in Kazakhstan. *Journal of Islamic Thought and Civilization, 15*(1), 166-84. https://doi.org/10.32350/jitc.151.10

Alazzam, F. A. F., & Aldrou, K. K. A. R. (2025). Artificial intelligence and data privacy in international trade law. *Multidisciplinary Science Journal, 7*(8), 2025379. https://doi.org/10.31893/multiscience.2025379

Alkhariji, L., De, S., Rana, O., & Perera, C. (2023). Semantics-based privacy by design for Internet of Things applications. *Future Generation Computer Systems*, 138, 280–295. https://doi.org/10.1016/j.future.2022.08.013

Anbari, K., Yousefvand, A. H., Qanadi, P., & Amraie, F. (2022). An investigation into the evaluation of the satisfaction with prenatal care services among pregnant women attending healthcare centers during pregnancy in the capital of Lorestan Province, Iran. *Advancements in Life Sciences, 9*(2), 224–230.

Beig, M. M., Ali, M. A., Javed, H., & Yaqub, T. (2024). Geospatial dynamics of SARS-CoV-2 variants during the Fifth Wave of COVID-19 in Punjab, Pakistan. *Advancements in Life Sciences, 11*(1), 45-58.

Bossi, M. (2021). Processing data to third countries or international organizations. *Arribat – International Journal of Human Rights, 1*(2), 176–186.

Council of Europe. (1981). Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108, as amended in 1999). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_121499/

Council of Europe. (1987). Recommendation No. R (87) 15 regulating the use of personal data in the police sector. Retrieved from https://rm.coe.int/168062dfd4

Council of Europe. (1991). Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies. Retrieved from https://rm.coe.int/cmrec-91-10-on-the-communication-to-third-parties-of-personal-data-hel/1680a43b60

Danelian, R. N., Yakovleva-Chernysheva, A. Yu., & Yakovlev-Chernyshev, V. A. (2023). Problems of legal certainty of legislative provisions in the sphere of legal protection of personal data. Vestnik Rossiiskoi pravovoi akademii, 3, 113–127.

Dmitrieva, E. G. (2021). Problems of personal data protection in the digital world and ways to solve them. Pravo i biznes, 3, 18–20.

Esmail, M., El-Dosuky, M. A., & Hamza, T. T. (2024). Solving problems of big data infrastructure by using blockchain. *Journal of Theoretical and Applied Information Technology, 102*(23), 1–18.

European Court of Human Rights. (1997). Z v. Finland, No. 22009/93. Retrieved from https://hudoc.echr.coe.int/eng?i=002-9432

European Court of Human Rights. (2002). Toma v. Romania, No. 42716/02. Retrieved from https://hudoc.echr.coe.int/eng?i=001-91513

European Court of Human Rights. (2003). Peck v. United Kingdom, No. 44647/98. Retrieved from https://hudoc.echr.coe.int/eng?i=001-60898

European Court of Human Rights. (2008). S and Marper v. United Kingdom, No. 30562/04. Retrieved from https://hudoc.echr.coe.int/eng?i=001-9005

European Court of Human Rights. (2015). R.E. v. Great Britain, No. 62498/11. Retrieved from https://hudoc.echr.coe.int/eng?i=001-158159

European Court of Human Rights. (2020). P.T. v. Moldova, No. 1122/12. Retrieved from https://hudoc.echr.coe.int/fre?i=001-202520

European Parliament & Council of the European Union. (1995). Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (repealed). Retrieved from https://base.garant.ru/2569783/

European Parliament & Council of the European Union. (2016). General Data Protection Regulation (GDPR) No. 2016/679. Retrieved from https://base.garant.ru/71936226/

Feng, D., Qin, Y., Feng, W., Li, W., Shang, K., & Ma, H. (2024). Survey of research on confidential computing. *IET Communications, 18*(9), 535–556. https://doi.org/10.1049/cmu2.12759

Gasiokwu, P. I., Oyibodoro, U. G., & Nwabuoku, M. O. I. (2025). GDPR Safeguards for Facial Recognition Technology: A Critical Analysis. *International Research Journal of Multidisciplinary Scope, 2025*(1), 45-60.

Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*, 1. https://doi.org/10.1016/j.csa.2023.100015

Keesal, C., Stathopoulou, A., & Gadzinski, G. (2025). Privacy perceptions and the role of countermeasures on the usage of in-app commerce. *Behaviour & Information Technology*, 1–24. https://doi.org/10.1080/0144929X.2025.2469657

Khoulimi, H., & Benammar, O. (2024). Optimized ANN Hyperparameters to Identify Malicious Traffic in Networks. *Journal of Theoretical and Applied Information Technology, 102*(22), 55-67.

Kohler, C. (2016). Conflict of law issues in the 2016 Data Protection Regulation of the European Union. Rivista di diritto internazionale privato e processuale, 653–675.

Krishnan, V. S., Bhatia, H., Khandal, H., & Vijayan, R. (2025). AI-Driven Early Skin Disease Detection: Skincare.ai's Impact and Efficacy. *International Research Journal of Multidisciplinary Scope, 2025*(1), 78-92.

Kurnianti, A. W., Prajarto, N., & Arymami, D. (2024). Between control and connection: The clash of dating apps and cultural norms in Indonesia. *Multidisciplinary Science Journal, 7*(6), 2025303. https://doi.org/10.31893/multiscience.2025303

Lachina, E. A., Kuznetsova, I. A., & Nosova, E. V. (2021). Problems of personal data protection on the Internet. *Uchenye zapiski, 1*(37), 116–121.

Lorincz, A. L. (2023). The Religious Oath in Judicial Proceedings from Romania Towards Replacing with a Secular Formula. *European Journal of Science and Theology, 19*(2), 45-60.

Mahdy, M., Hartiwiningsih, & Isharyanto. (2025). Wiretapping law in Indonesia: Realising due process of law. *Multidisciplinary Science Journal*, (Accepted Articles). Retrieved from https://malque.pub/ojs/index.php/msj/article/view/7844

Marelli, M. (2024). Transferring personal data to international organizations under the GDPR: An analysis of the transfer mechanisms. *International Data Privacy Law, 14*(1), 19–36.

Navarro-Hernández, J. L. (2022). Analysis of judicial control prior to actions that limit the fundamental right to privacy in Colombia. *JURIDICAS CUC, 18*(1), 279–302. https://doi.org/10.17981/juridcuc.18.1.2022.12.

Neznamova, A. A., Kuleshov, G. N., & Turkin, M. M. (2020). International experience in personal data protection. *JURIDICAS CUC, 16*(1), 391–406. https://doi.org/10.17981/juridcuc.16.1.2020.17

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. *Computer Law & Security Review*, 55. https://doi.org/10.1016/j.clsr.2024.106066

Nuffield Council on Bioethics. (2007). The forensic use of bioinformation: Ethical issues (p. 139). Retrieved from https://www.statewatch.org/media/documents/news/2007/sep/uk-nuffield-bioinformation-summary.pdf

Petrov, A., Mirzagitova, A., Kuraev, A., & Kirillova, E. (2024). Main threats to human rights and freedoms in the context of digitalization. *JURIDICAS CUC, 20*(1), 343–357. https://doi.org/10.17981/juridcuc.20.1.2024.16

Pop, M. R., & Pop, C. M. (2023). Exploring the influence of religious service characteristics on parishioners' overall satisfaction in Protestant church. *European Journal of Science and Theology, 19*(2), 85-97.

Rupp, V., & von Grafenstein, M. (2024). Clarifying "personal data" and the role of anonymisation in data protection law including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection. *Computer Law and Security Review*, 52. https://doi.org/10.1016/j.clsr.2023.105932

Russian Federation. (2006). Federal Law "On Personal Data" No. 152-FZ (latest edition). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_61801/

Semenov, E. Yu., & Lysenko, E. S. (2021). Problems of legal regulation of automated processing of publicly available personal data. *Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii*, (1), 47–52.

Søe, S.O., Jørgensen, R.F. & Mai, JE. (2021). What is the 'personal' in 'personal information'? *Ethics and Information Technology*, 23, 625–633 https://doi.org/10.1007/s10676-021-09600-3

T-Trang Lâm. (2024). Some legal aspects of personal data protection in the world – Experience for Vietnam. *Cogent Social Sciences, 10*(1), 2414872. https://doi.org/10.1080/23311886.2024.2414872

Uvizheva, A. V., Koibaev, B. G., & Pekh, A. A. (2020). Problems of personal data protection in the information policy of the Russian Federation. Teorii i problemy politicheskikh issledovanii, 9(5A), 146–154.

Vasyukov, V. F. (2021) Investigation and seizure of electronic media in the production of investigative actions. *Revista de Direito, Estado e Telecomunicacoes, 13*(2), 78-88. https://doi.org/10.26512/lstr.v13i2.25920.

FINANCING

Research hasn't received any financing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

CONTRIBUTION AND CREDIT

Conceptualización, ideas y la evolución del diseño del trabajo: Elvir Akhmetshin
Obtención, revisión y análisis de los datos o categorías: Nazgul Ibrayeva
Escritura y presentación del artículo: Mukhabbatkhon Agzamova, Ilyos Abdullayev

Revisión crítica del contenido del manuscrito: Aleksandr Kiselev

BIODATA

Nazgul Ibrayeva is a graduate student at the Higher School of Law, Astana International University. Her research interests focus on the development of legal institutions and human rights protection.

Mukhabbatkhon Agzamova is affiliated with the International Islamic Academy of the Republic of Uzbekistan, Tashkent. Her academic interests lie in international law and the interaction between state and religion in legal systems.

Ilyos Abdullayev is Doctor of Economic Sciences and Professor, serving as Dean of the Faculty of Social and Economic Sciences at the Department of Business and Management of Urgench State University. His research interest covers economic policy, higher education management, and comparative development studies.

Elvir Akhmetshin. Candidate of Economic Sciences, Associate Professor. Head of Department of Science, Innovation and Technology, Associate Professor of Department of Economics Mamun University, Uzbekistan.

Aleksandr Kiselev holds a PhD in Law and is Leading Researcher at the Center for Research and Expertise, as well as Associate Professor in the Department of International and Public Law at the Financial University under the Government of the Russian Federation. His research focuses on constitutional law, international legal frameworks, and the protection of human rights.