



ANALYSIS OF THE OBJECTIVE ELEMENTS OF THE OFFENCE AGAINST THE INVIOABILITY OF PRIVATE LIFE (ON THE EXAMPLE OF ARTICLE 141¹ OF THE CRIMINAL CODE OF THE REPUBLIC OF UZBEKISTAN)

Bozorov Jasurbek Saydulla o'g'li

Basic doctoral student, Academy of Justice of the Republic of
Uzbekistan, specialisation "12.00.08 — Criminal Law. Criminology.
Criminal Enforcement Law"

Tel.: +998 94 338 69 99. E-mail: jasurbekkbozorovqash@gmail.com
<https://doi.org/10.5281/zenodo.22143968>

Abstract. The article provides a systematic analysis of the objective elements — the object, the subject matter and the actus reus — of the offence of violation of the inviolability of private life under Article 141¹ of the Criminal Code of the Republic of Uzbekistan. Relying on the vertical classification of the object of the offence (general, generic and immediate), the author argues that the immediate object consists of social relations in the sphere of the exercise of the right to privacy enshrined in Article 31 of the Constitution. The analysis of the actus reus covers the two alternative forms of conduct — the unlawful collection and the unlawful dissemination of information, their content and mutual delimitation, the moment of completion of the offence, the constitutive role of administrative prejudice, and the circumstances excluding the criminality of the act. The analysis identifies six systemic mismatches between the constitutional guarantee and the scope of criminal-law protection, and formulates six proposals, including two draft provisions and a draft clause of a resolution of the Plenum of the Supreme Court.

Keywords: privacy, object of the offence, subject matter of the offence, actus reus, administrative prejudice, qualifying element, special categories of personal data, dissemination of information, Article 141¹ of the Criminal Code, Article 31 of the Constitution.

Annotatsiya. Maqolada O'zbekiston Respublikasi Jinoyat kodeksining 141¹-moddasida nazarda tutilgan shaxsiy hayot daxlsizligini buzish jinoyatining obyektiv belgilari — jinoyat obyekti, jinoyat predmeti va jinoyatning obyektiv tomoni tizimli tarzda tahlil qilingan. Jinoyat obyektini vertikal tasniflash (umumiy, turdosh, bevosita obyekt) asosida mazkur tajovuzning bevosita obyekti Konstitutsiyaning 31-moddasida mustahkamlangan shaxsiy hayot daxlsizligi huquqini ro'yobga chiqarish sohasidagi ijtimoiy munosabatlardan iborat ekanligi asoslangan. Obyektiv tomon tahlilida qilmishning ikki muqobil shakli — ma'lumotlarni qonunga xilof ravishda yig'ish hamda tarqatish, ularning mazmuni va o'zaro chegarasi, jinoyatning tugallangan payti, ma'muriy preyditsiyaning tarkib hosil qiluvchi ahamiyati va qilmishning jinoiyligini istisno etuvchi holatlar o'rganilgan. Tahlil natijasida konstitutsiyaviy kafolat bilan jinoiy-huquqiy himoya doirasi o'rtasidagi oltita tizimli nomuvofiqlik aniqlanib, ularni bartaraf etishga qaratilgan oltita taklif, shu jumladan ikkita norma loyihasi va Oliy sud Plenumi qarori bandining loyihasi ishlab chiqilgan.

Kalit so'zlar: shaxsiy hayot daxlsizligi, jinoyat obyekti, jinoyat predmeti, obyektiv tomon, ma'muriy preyditsiya, malakalovchi belgi, shaxsga doir maxsus ma'lumotlar, ma'lumotlarni tarqatish, Jinoyat kodeksining 141¹-moddasi, Konstitutsiyaning 31-moddasi.

Аннотация. В статье системно проанализированы объективные признаки состава нарушения неприкосновенности частной жизни, предусмотренного статьёй 141¹

Уголовного кодекса Республики Узбекистан, — объект, предмет и объективная сторона преступления. На основе вертикальной классификации объекта (общий, родовой, непосредственный) обосновано, что непосредственным объектом посягательства выступают общественные отношения в сфере реализации права на неприкосновенность частной жизни, закреплённого статьёй 31 Конституции. При анализе объективной стороны рассмотрены две альтернативные формы деяния — незаконное собирание и распространение сведений, их содержание и взаимное разграничение, момент окончания преступления, составообразующее значение административной преюдиции, а также обстоятельства, исключающие преступность деяния. По результатам анализа выявлено шесть системных несоответствий между конституционной гарантией и пределами уголовно-правовой охраны и разработано шесть предложений, включая два проекта норм и проект пункта постановления Пленума Верховного суда.

Ключевые слова: неприкосновенность частной жизни, объект преступления, предмет преступления, объективная сторона, административная преюдиция, квалифицирующий признак, специальные персональные данные, распространение сведений, статья 141¹ УК, статья 31 Конституции.

Introduction

Under Article 31 of the Constitution of the Republic of Uzbekistan, everyone has the right to the inviolability of private life, to personal and family secrecy and to the protection of his or her honour and dignity; everyone has the right to the secrecy of correspondence, telephone conversations, postal, electronic and other communications, as well as the right to the protection of personal data relating to him or her¹. This provision was qualitatively renewed as a result of the constitutional reform of 2023: instead of the earlier formula on “protection against interference with private life”, the rights to the protection of personal data, to the rectification of inaccurate data and to demand the destruction of unlawfully collected data were separately entrenched. This has brought the constitutional standard for safeguarding the inviolability of private life closer to international requirements.

At the international level this guarantee is expressed in Article 17 of the International Covenant on Civil and Political Rights of 1966 — as the prohibition of arbitrary or unlawful interference with anyone’s private and family life². In national legislation it is developed by Article 13 of the Law “On the Principles and Guarantees of Freedom of Information”³ and by the provisions of the Law “On Personal Data”⁴.

The criminal-law mechanism of this guarantee was established by Law No. ZRU-411 of 23 September 2016: the Criminal Code was supplemented with Article 141¹ (“Violation of the

¹Constitution of the Republic of Uzbekistan (version adopted at the national referendum of 30 April 2023). Article 31 // National Database of Legislation, 1 May 2023, No. 03/23/837/0241. — <https://lex.uz/docs/-6445145>

²International Covenant on Civil and Political Rights (New York, 16 December 1966). Article 17. The Republic of Uzbekistan acceded to the Covenant in 1995.

³Law of the Republic of Uzbekistan “On the Principles and Guarantees of Freedom of Information”, 12 December 2002, No. 439-II. Article 13 // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 2003, No. 1, Art. 2. — <https://lex.uz/acts/-52268>

⁴Law of the Republic of Uzbekistan “On Personal Data”, 2 July 2019, No. ZRU-547. Articles 3 and 25. — <https://lex.uz/docs/-4396419>

inviolability of private life”), and the Code on Administrative Responsibility with Article 46¹⁵. A two-tier model of liability based on administrative prejudice was thereby introduced into national law.

The relevance of the topic is explained by two factors. First, in the digital environment the forms of intrusion into private life (covert video recording, geolocation tracking, false images generated by artificial intelligence) are changing rapidly, whereas the disposition of Article 141¹ has remained unaltered since 2016. Second, it is precisely the objective elements of the corpus delicti that are decisive for the legal characterisation of the act and for delimiting it from an administrative offence and from adjacent corpora delicti (Articles 141², 142 and 143 of the Criminal Code).

The aim of the study is to clarify, at the doctrinal level, the objective elements of the corpus delicti provided for in Article 141¹ of the Criminal Code, to identify the mismatches between those elements and the guarantee contained in Article 31 of the Constitution, and to develop concrete normative proposals for eliminating them.

The scholarly justification of the inviolability of private life as an independent legal value begins with the celebrated article published by S. Warren and L. Brandeis in 1890, in which the right in question was defined as “the right to be let alone”⁶. A. Westin subsequently interpreted privacy as the individual’s ability to control information about himself or herself, thereby laying the foundation of the concept of informational privacy⁷. Today this approach forms the theoretical core of personal data protection.

In post-Soviet legal scholarship, Ye.A. Filimonova characterises the right to the inviolability of private life as a two-layered construction: on the one hand, the individual’s natural right to self-determination and to protection against unjustified interference by the State, society or third parties; on the other hand, a legal category consisting of a body of powers guaranteed by the State⁸. This approach is important for criminal-law analysis: it makes it possible to view the immediate object not as a single but as a complex social relation.

At the same time, in national criminal-law doctrine the objective elements of Article 141¹ in particular — the boundaries of the subject matter of the offence, the content of the notions of “collection” and “dissemination”, and the constitutive role of administrative prejudice — have not been examined at monographic level. The majority of the existing works are devoted to constitutional and civil-law aspects, while criminal-law analysis is, as a rule, confined to a general commentary on the article. The present article seeks to fill that gap.

The study employs the dogmatic-legal method (interpretation of the norm in terms of its text and content), the systemic-structural method (examination of the elements of the corpus delicti in their interconnection), the formal-juridical method (clarification of legal concepts)

⁵Law of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan”, 23 September 2016, No. ZRU-411 (introducing Article 141¹ into the Criminal Code and Article 46¹ into the Code of Administrative Responsibility). — <https://lex.uz/docs/-3033167>

⁶Warren S.D., Brandeis L.D. The Right to Privacy // Harvard Law Review. — 1890. — Vol. 4, No. 5. — P. 193–220.

⁷Westin A.F. Privacy and Freedom. — New York: Atheneum, 1967.

⁸Филимонова Е.А. Конституционное право российских граждан на неприкосновенность частной жизни: Дис. ... канд. юрид. наук. — Волгоград, 2005. — С. 34. [The page of the citation is to be re-verified by the author against the original.]

and the comparative-legal method. The normative basis is formed by the Constitution of the Republic of Uzbekistan, the Criminal Code, the Criminal Procedure Code, the Code on Administrative Responsibility, and the Laws "On the Principles and Guarantees of Freedom of Information" and "On Personal Data". For the purposes of comparative analysis, the relevant provisions of the criminal codes of France, Germany, the Russian Federation and the Republic of Kazakhstan have been drawn upon, together with the rules of Convention No. 108 of the Council of Europe and Regulation (EU) 2016/679 (GDPR).

Main part

In accordance with Article 14 of the Criminal Code, a socially dangerous act (action or omission) committed with fault and prohibited by the Criminal Code under threat of punishment is recognised as an offence⁹. The corpus delicti is understood as the aggregate of objective and subjective elements necessary and sufficient for a specific socially dangerous act to be assessed as an offence. Two of its four elements — the object of the offence and the *actus reus* — form the group of objective elements; the subject matter of the offence appears as a facultative feature of the object which is, however, mandatory for the purposes of Article 141¹.

The object of the offence is the social relation protected by criminal law which is harmed, or placed in danger of being harmed, as a result of the commission of the offence. The range of protected values is expressed in Article 2 of the Criminal Code and in the titles of the divisions and chapters of the Special Part¹⁰.

Applying the vertical classification, the objects of the intrusion under analysis are determined as follows:

- the general object — the aggregate of all social relations protected by criminal law;
- the generic object — social relations in the sphere of the exercise of the constitutional rights and freedoms of citizens (the corresponding chapter of the Special Part of the Criminal Code);
- the immediate object — social relations in the sphere of the exercise of the right to the inviolability of private life and to personal and family secrecy, enshrined in Article 31 of the Constitution.

Defining the immediate object in precisely this way has practical significance: it provides the criterion for delimiting Article 141¹ from Article 141² of the Criminal Code (whose immediate object is the established procedure for the processing of personal data), from Article 142 (inviolability of the home) and from Article 143 (the regime of secrecy of communications). It must be emphasised, however, that the scope of the guarantee under Article 31 of the Constitution is broader than the actual protective reach of Article 141¹ — an issue considered below as a problem.

The subject matter of the offence consists of information about a person's private life which constitutes his or her personal or family secret and which may not be disclosed without that person's consent¹¹. The subject matter covers not only information that discredits the person or his or her family, but also any other information which the person wishes to keep confidential: illness of a family member, romantic relationships, financial situation, religious

⁹Criminal Code of the Republic of Uzbekistan, 22 September 1994. Article 14. — <https://lex.uz/docs/-111453>

¹⁰Criminal Code of the Republic of Uzbekistan, 22 September 1994. Article 2. — <https://lex.uz/docs/-111453>

¹¹Criminal Code of the Republic of Uzbekistan, 22 September 1994. Article 141¹. — <https://lex.uz/docs/-111453>



belief and so forth. The decisive criterion is not the objectively “shameful” character of the information, but the existence of a subjective yet lawful interest in keeping it secret.

In determining the subject matter, Article 25 of the Law “On Personal Data” serves as an important reference point: according to it, information on racial or social origin, political, religious or philosophical convictions, information relating to physical or mental health, information on private life and on criminal record constitute special categories of personal data, and their processing is prohibited as a general rule¹². This demonstrates that, as the subject matter of an offence, such data require a higher level of protection.

The *actus reus* is the aggregate of legally significant features characterising the external manifestation of a socially dangerous intrusion directed against an object protected by criminal law. It is precisely the features of the *actus reus* that are expressed most fully, as compared with the other elements, in the dispositions of the articles of the Special Part; for that reason they constitute the principal criterion for distinguishing offences from one another and for their legal characterisation.

The *actus reus* of the offence under analysis is characterised by two alternative forms of conduct:

- (a) the unlawful collection, without the person’s consent, of information about his or her private life constituting a personal or family secret;
- (b) the unlawful dissemination of such information.

Collection is understood to mean any acts directed at obtaining the information: surveillance of the person, following him or her, taking photographs or video recordings, making enquiries of persons who know him or her, examining documents, copying from electronic sources and the like. The determining factor is the absence of the consent of the person to whom the information relates, since it is for that person alone to decide which part of the information is to be kept secret.

Dissemination is understood to mean communicating the information to at least one third party: publication in the mass media, posting on the Internet, disclosure before an audience, sending a message. In practice the method of dissemination does not affect the legal characterisation, but it must be taken into account in sentencing, since dissemination via the Internet leads to the irreversible publicity of the information.

An important aspect is that, where the information has become known to the public through the victim’s own conduct (for example, where the person is regularly seen in a state of intoxication by those living around his or her place of residence), the information loses its confidential character and the subject matter of the offence is absent — and consequently there is no *corpus delicti* either.

The second mandatory feature of the *actus reus* is administrative prejudice. According to the disposition of Article 141¹, liability arises only in respect of an act committed after an administrative penalty has been imposed for the same conduct¹³; the initial act entails

¹²Law of the Republic of Uzbekistan “On Personal Data”, 2 July 2019, No. ZRU-547. Article 25. — <https://lex.uz/docs/-4396419>

¹³Criminal Code of the Republic of Uzbekistan, 22 September 1994. Article 141¹. — <https://lex.uz/docs/-111453>

administrative liability under Article 46¹ of the Code on Administrative Responsibility¹⁴. Accordingly, the fact that an administrative penalty has been imposed, and the period during which it remains in force, constitute a necessary condition of the *corpus delicti*; where that fact is not proved, the act cannot be characterised as an offence.

As regards the moment at which the offence is completed, the views expressed in the literature are divergent. Taking into account that the *corpus delicti* is a formal one, the following position is submitted: the offence is completed from the moment at which the act of collecting or disseminating the information is committed after the imposition of the administrative penalty; the occurrence of a socially dangerous consequence is not a necessary element of the *corpus delicti*. Acts directed at collection which have ended without result should be assessed as an attempt to commit the offence. The formula encountered in the current literature, according to which the offence “is completed from the moment collection begins”, is not well founded, since it conflates a completed offence with an attempt.

Finally, the unlawfulness of the act is a necessary element of the *corpus delicti*. Where the collection or dissemination of information is based on legislation — for example, where it is carried out in accordance with the legislation on operational-search activity, with the Criminal Procedure Code or with the legislation on the mass media — the act is not recognised as an offence. Even within the framework of procedural activity, the prohibition contained in part three of Article 17 of the Criminal Procedure Code applies: it is prohibited to perform acts or to adopt decisions that degrade a person’s honour and dignity or that lead to the dissemination of information relating to his or her private life¹⁵.

Foreign experience demonstrates alternative models for constructing the objective elements. Article 226-1 of the French Criminal Code links the intrusion into the privacy of private life to the very fact of recording or capturing an image without consent, without requiring the information to constitute a “secret”¹⁶. Section 201a of the German Criminal Code provides for an independent *corpus delicti* for intrusion, by means of image recording, into the most intimate sphere of private life, and treats the image as an independent subject matter¹⁷. Article 137 of the Criminal Code of the Russian Federation and Article 147 of the Criminal Code of the Republic of Kazakhstan, for their part, establish a system of qualifying elements such as the use of official position and public dissemination, without requiring administrative prejudice¹⁸. Convention No. 108 of the Council of Europe¹⁹ and Article 9 of the GDPR²⁰ establish

¹⁴Code of the Republic of Uzbekistan on Administrative Responsibility, 22 September 1994. Article 46¹. — <https://lex.uz/acts/-97664>

¹⁵Criminal Procedure Code of the Republic of Uzbekistan, 22 September 1994. Article 17, part three. — <https://lex.uz/docs/-111460>

¹⁶Code pénal de la République française. Art. 226-1 (atteinte à l’intimité de la vie privée).

¹⁷Strafgesetzbuch der Bundesrepublik Deutschland. § 201a (Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen).

¹⁸Уголовный кодекс Российской Федерации. Ст. 137; Уголовный кодекс Республики Казахстан. Ст. 147.

¹⁹Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). — Strasbourg, 28.01.1981; Protocol CETS No. 223 (2018).

²⁰Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Art. 9.



a reinforced regime for special categories of data, while the case-law of the European Court of Human Rights resolves the conflict between private life and freedom of expression through the “public interest” test²¹.

First problem. The narrowness of the immediate object and of the subject matter as compared with the constitutional guarantee.

The disposition of Article 141¹ confines protection to information alone that “constitutes a personal or family secret”. Article 31 of the Constitution, however, guarantees the inviolability of private life more broadly — in a manner that also covers information which does not have the status of a secret but nevertheless relates to private life (image, voice, location data, daily movement routes). As a result, the intrusions most frequently encountered in the digital environment — covert video recording without consent, geolocation tracking, and false images generated by artificial intelligence — remain outside criminal-law protection.

First proposal. To replace the words “constituting a personal or family secret” in the disposition of Article 141¹ with the words “relating to private life”, and to include within the subject matter, by way of an enumeration, information about a person’s image, voice and location (geolocation).

Third problem. The absence of a developed system of qualifying elements.

Article 141¹ consists of a single part, and the sharp differences in the degree of social danger are not reflected at all in the measures of punishment. This has an adverse effect on the individualisation of punishment and on the principle of justice.

Third proposal (draft provision No. 1). To supplement Article 141¹ with a second and a third part in the following terms:

“The same acts, where they are committed: (a) through the mass media or telecommunications networks, including the Internet global information network; (b) out of self-interested or other base motives; (c) with the use of official position; (d) in respect of a minor, — shall entail liability irrespective of the condition, provided for in part one of this Article, that they be committed after the imposition of an administrative penalty.”

“The acts provided for in part one or part two of this Article, where they have caused grave consequences, — ...”

Fourth problem. The lack of differentiation in the protection of special categories of personal data.

Article 25 of the Law “On Personal Data” classifies as a special category information relating to health, criminal record, religious and political convictions, and racial and social origin, and prohibits the processing of such data as a general rule. Articles 141² and 141¹ of the Criminal Code, however, do not reflect that differentiation — an intrusion in respect of special data is assessed in the same way as an intrusion in respect of ordinary data²². This constitutes a departure from the standards of Article 9 of the GDPR and of Convention No. 108.

²¹ECtHR, *Von Hannover v. Germany*, no. 59320/00, judgment of 24 June 2004; ECtHR [GC], *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04, judgment of 4 December 2008.

²²Criminal Code of the Republic of Uzbekistan, 22 September 1994. Article 141²; Code of the Republic of Uzbekistan on Administrative Responsibility. Article 46².

Fourth proposal (draft provision No. 2). To introduce into Article 141² a qualifying element in the following terms: “the same acts, where they are committed in respect of special categories of personal data, —”, and to establish a heightened punishment.

Fifth problem. The normative indeterminacy of the notions of “collection” and “dissemination”.

Neither the legislation nor the instruments guiding judicial practice disclose the content of the notions of “collection” and “dissemination”. In particular, the questions whether communicating information to a single third party amounts to dissemination, and from what moment collection is to be regarded as completed, remain unresolved. In practice this leads to inconsistent legal characterisation.

Fifth proposal. To supplement the relevant resolution of the Plenum of the Supreme Court with a clause in the following terms: “It shall be explained to the courts that the collection of information within the meaning of Article 141¹ of the Criminal Code means any act directed at obtaining it (surveillance, image recording, audio recording, making enquiries of third parties, copying from electronic sources), and that the offence is completed from the moment the information is actually obtained. The dissemination of information means communicating it to at least one third party; the method of dissemination does not affect the legal characterisation but shall be taken into account in the imposition of punishment.”

Sixth problem. The absence of a criterion for resolving conflicts of rights.

Where the inviolability of private life comes into conflict with freedom of speech and of the mass media, national law lays down no criteria for assessing the lawfulness of the act. The element of unlawfulness is formulated in blanket terms, and the court is compelled to rely on its own discretion.

Sixth proposal. To entrench the “public interest” test in a resolution of the Plenum of the Supreme Court: to establish that the dissemination of information should not be found unlawful where it serves the discussion of a matter of significance for society, where the volume of the information disseminated is proportionate to that purpose, and where the victim is a person performing a public function. In doing so, the proportionality approach adopted by the European Court of Human Rights in the Von Hannover and S. and Marper cases may be used as a comparative source.

Conclusion

On the basis of the analysis carried out above, the following conclusions may be drawn.

First, the immediate object of the offence provided for in Article 141¹ of the Criminal Code consists of social relations in the sphere of the exercise of the right to the inviolability of private life and to personal and family secrecy, enshrined in Article 31 of the Constitution; this criterion makes it possible to delimit that Article from Articles 141², 142 and 143 of the Criminal Code.

Second, the decisive factor in determining the subject matter of the offence is not the objectively “shameful” character of the information but the existence of a lawful interest in keeping it secret; where the information has become public through the victim’s own conduct, there is no subject matter and, consequently, no *corpus delicti*.

Third, the *actus reus* is characterised by two alternative forms of conduct (collection and dissemination) and by the mandatory element of administrative prejudice; the offence has a formal *corpus delicti* and is regarded as completed from the moment the act is committed following the imposition of an administrative penalty.

Fourth, there are five systemic mismatches between the constitutional guarantee and the scope of criminal-law protection, which manifest themselves in the narrowness of the subject matter, the absence of a system of qualifying elements, the lack of differentiation in the protection of special categories of data, the normative indeterminacy of the key notions, and the absence of a criterion for resolving conflicts of rights.

Fifth, in order to eliminate these mismatches, two draft provisions (a new part two and part three of Article 141¹ of the Criminal Code, and a qualifying element concerning special categories of data in Article 141²) and two draft clauses of a resolution of the Plenum of the Supreme Court have been proposed. Their adoption would serve to bring the criminal law into conformity with the requirements of Article 31 of the Constitution and with the international standards of personal data protection.

List of references:

1. Constitution of the Republic of Uzbekistan (version adopted at the national referendum of 30 April 2023) // National Database of Legislation, 1 May 2023, No. 03/23/837/0241. — <https://lex.uz/docs/-6445145>
2. International Covenant on Civil and Political Rights (New York, 16 December 1966).
3. Criminal Code of the Republic of Uzbekistan, 22 September 1994. — <https://lex.uz/docs/-111453>
4. Criminal Procedure Code of the Republic of Uzbekistan, 22 September 1994. — <https://lex.uz/docs/-111460>
5. Code of the Republic of Uzbekistan on Administrative Responsibility, 22 September 1994. — <https://lex.uz/acts/-97664>
6. Law of the Republic of Uzbekistan "On the Principles and Guarantees of Freedom of Information", 12 December 2002, No. 439-II // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 2003, No. 1, Art. 2. — <https://lex.uz/acts/-52268>
7. Law of the Republic of Uzbekistan "On Personal Data", 2 July 2019, No. ZRU-547. — <https://lex.uz/docs/-4396419>
8. Law of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan", 23 September 2016, No. ZRU-411. — <https://lex.uz/docs/-3033167>
9. Code pénal de la République française. Art. 226-1.
10. Strafgesetzbuch der Bundesrepublik Deutschland. § 201a.
11. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. Ст. 137.
12. Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V. Ст. 147.
13. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). — Strasbourg, 28.01.1981; Protocol CETS No. 223 (2018).
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR). Art. 9.
15. ECtHR, Von Hannover v. Germany, no. 59320/00, judgment of 24 June 2004.
16. ECtHR [GC], S. and Marper v. the United Kingdom, nos. 30562/04 and 30566/04, judgment of 4 December 2008.
17. Warren S.D., Brandeis L.D. The Right to Privacy // Harvard Law Review. — 1890. — Vol. 4, No. 5. — P. 193–220.

18. Westin A.F. Privacy and Freedom. — New York: Atheneum, 1967. — 487 p.

19. Филимонова Е.А. Конституционное право российских граждан на неприкосновенность частной жизни: Дис. ... канд. юрид. наук. — Волгоград, 2005. — 34 с.