

Legal regulation of profiling and targeted advertising in Kazakhstan through the lens of European experience

Saule Akhmetova*

PhD in Law
Al-Farabi Kazakh National University
050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan
<https://orcid.org/0009-0004-5393-4752>

Alua Ibrayeva

Doctor of Law, Professor
Al-Farabi Kazakh National University
050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan
<https://orcid.org/0000-0002-2946-6408>

Dina Baimakhanova

Doctor of Law, Associate Professor
Al-Farabi Kazakh National University
050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan
<https://orcid.org/0000-0001-5903-9020>

Dinara Tursynkulova

PhD in Law, Associate Professor
Al-Farabi Kazakh National University
050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan
<https://orcid.org/0000-0003-4768-2048>

Thomas Hoffmann

Doctor of Law, Associate Professor
Tallinn University of Technology
19086, 5 Ehitajate tee, Tallinn, Estonia
<https://orcid.org/0000-0003-4761-0722>

Abstract. The study was dedicated to analysing the current legal framework regulating profiling and targeted advertising in Kazakhstan, considering the European experience. The study involved a review of regulations of Kazakhstan governing the use of personal data and a comparative analysis with the provisions of General Data Protection Regulation. The analysis demonstrated that while Kazakhstan has established basic standards for the protection of personal data, the level of transparency and control over the data processing process remains noticeably lower compared to European norms. The main issues included the lack of explicit user consent for the use of their data for targeted advertising, limited opportunities for managing personal information, and insufficient financial resources for employing advanced technologies and certain legal restrictions caused by stringent state policies. An examination of Kazakhstani online platforms, including examples such as Kaspi, Tengrinews, and Krisha, demonstrated that data processing procedures on these platforms do not comply with the standards of the General Data Protection Regulation. This creates legal risks for businesses, particularly in relation to potential entry into the European market. The findings of the study highlighted the necessity of improving national legislation in the field of personal data protection. It was recommended to introduce mechanisms ensuring explicit user consent for data processing, enhance the transparency of privacy policies, and expand user rights, including the ability to

Suggested Citation

Article's History: Received: 25.11.2024 Revised: 26.02.2025 Accepted: 26.03.2025

Akhmetova, S., Ibrayeva, A., Baimakhanova, D., Tursynkulova, D., & Hoffmann, T. (2025). Legal regulation of profiling and targeted advertising in Kazakhstan through the lens of European experience. *Social & Legal Studios*, 8(1), 33-45. doi: 10.32518/sals1.2025.33.

*Corresponding author



delete stored data and transfer it. Aligning the legislation of Kazakhstan with European standards will not only strengthen the protection of citizens' rights but also increase the competitiveness of Kazakhstani companies in the international arena

Keywords: personal data processing; international standards; privacy policy; digital market; user rights protection

Introduction

In the era of the digital economy, data has become a new valuable asset, and its commercial use is gaining increasing importance. Profiling and targeted advertising, as key tools of digital marketing, enable companies to tailor advertising messages based on the analysis of user behaviour and preferences. These methods play a crucial role in shaping market strategies and enhancing business efficiency but also raise serious concerns about personal data protection and consumer rights compliance.

In the context of globalisation and the rapid development of information technologies, many countries face the need to establish laws to regulate data processing in profiling and targeted advertising (Maulenov *et al.*, 2024). The General Data Protection Regulation (GDPR) (2016), introduced by the European Union, has set high standards for personal data protection, which have become a model for many countries. As global digital integration progresses, the possibility for Kazakhstani internet platforms to enter the European market is growing in importance (Nurbatyrova *et al.*, 2024). The expansion of Kazakhstani platforms into European markets is essential for fostering international business relationships and tapping into a larger consumer base. As Kazakhstan works to bring its standards into line with those of Europe, it is clear that significant reform is required to the nation's data protection laws, especially with regard to profiling and targeted advertising (Zhetpissov *et al.*, 2024). Companies in Kazakhstan may be exposed to legal risks due to the discrepancy between the EU's demanding standards and Kazakhstan's present rules. Failure to comply with these standards may result in penalties and restrictions (Yerbolatov *et al.*, 2022). In addition to being a question of legal compliance, harmonising Kazakhstan's data protection regulations with the GDPR is strategically necessary to increase Kazakhstani businesses' competitiveness globally. The country's digital economy will eventually gain from this alignment since it will give Kazakhstani companies access to the European market, boost customer confidence, and enhance data processing transparency generally.

The dissemination and implementation of European standards for regulating data protection issues in legal contexts has received considerable attention in academic circles. For instance, G. Gentile and O. Lynskey (2022) explored this issue in detail, analysing challenges associated with the transnational application of the GDPR and criticising the current system of GDPR enforcement at the international level, which complicates its effective implementation across different countries. International legal aspects of these issues were also examined by R.D. Veit (2022), who conducted a comparative analysis of approaches in various European countries such as Germany. Similarly, B.C. Prokk and I. Schneider (2021) concluded that the GDPR plays an important geopolitical role, influencing international data regulation norms and reinforcing the EU's leading position in the field of personal information protection.

There are also studies specifically focused on the application of these standards in Central Asia. For example, K. Chan *et al.* (2022) examined the legal regimes governing

data regulation in Kazakhstan and Uzbekistan, in comparison with China, other countries, and major technology companies (Big Tech). They highlighted how, in the context of increasing digital control and authoritarian regimes, the legislation of Central Asian countries affects user freedoms and rights to privacy. The study also addresses the challenges of complying with global regulations such as the GDPR in the region, using examples of the operations of major technology companies (such as Google, Facebook, and others) within these countries. A. Younas *et al.* (2020) analysed the existing regulatory frameworks in Central Asian countries such as Kazakhstan, Uzbekistan, Kyrgyzstan, and Tajikistan, evaluating how these nations adapt to global trends in the processing of big data and cloud technologies. The authors examined how the countries in the region implement laws regulating the storage and processing of data in the cloud and assess the extent to which these laws align with international standards such as the GDPR. M. Toqmadi and N. Zakharchenko (2021) explored how users in Central Asia engage with issues of online privacy and consent to terms of data usage, often without any clear understanding of the essence of privacy policies or their rights. M. Lukings and A.H. Lashkari (2022), in their study on data sovereignty and cybersecurity, provided examples of international practices and noted that since the summer of 2020, Kazakhstan has begun adapting its laws to meet GDPR requirements. In their view, this demonstrates the country's ambition to modernise data protection legislation, enhance data security levels, build citizens' trust in digital services, and align the legal system with international standards.

The academic community has also produced research specifically focused on analysing the legal framework of Kazakhstan. Among the researchers who addressed this issue are Y.Y. Yerbolatov *et al.* (2022), who conducted a comparative analysis of personal data protection regulations in Kazakhstan and the European Union, with a particular focus on the GDPR. Similarly, Zh.T. Iskakova and T.S. Kadyrzhanova (2022) addressed the challenges and issues associated with the legislation of Kazakhstan on personal data protection, examining its compliance with international standards, including the GDPR. All the aforementioned authors agree that the personal data protection legislation of Kazakhstan falls short of many international standards, resulting in gaps in safeguarding citizens' rights. They also highlighted a number of key issues, the most noteworthy of which include the absence of clear regulations governing the transfer of data abroad (creating problems in the context of global digitalisation), limited awareness of privacy threats, a lack of understanding among users regarding the risks associated with the use of their personal data (including for targeting and profiling), low levels of digital literacy among internet users, inadequacies in the legislation of Kazakhstan, and challenges in implementing GDPR-equivalent standards. These issues are further exacerbated by limited transparency in data processing and insufficient enforcement mechanisms.

The purpose of this study was to identifying shortcomings in the legal regulation of profiling and targeted

advertising in Kazakhstan from the perspective of the European experience. The objectives of the study focused on identifying existing legal gaps and issues in national regulation and developing recommendations for improving legislation in accordance with international standards.

Materials and methods

The first stage of the study involved an analysis of the legislation of Kazakhstan regulating profiling and targeted advertising. Key regulations are examined, including the Law of the Republic of Kazakhstan No. 94-5 “On Personal Data and their Protection” (2013), as well as other legislative documents such as the Law of the Republic of Kazakhstan No. 508-2 “On Advertising” (2003) and the Law of the Republic of Kazakhstan No. 18-8 “On Online Platforms and Online Advertising” (2023). This analysis aimed to identify the key provisions ensuring the protection of users’ rights and limiting the misuse of their data in the context of profiling and targeted advertising. Subsequently, the legislation of Kazakhstan is compared with the provisions of the European General Data Protection Regulation (GDPR) (2016), which serves as an international standard in personal data protection.

The methodology included an analysis of the key provisions of the legislation of Kazakhstan and the European Union. The following elements of legal regulation are selected for comparison: the definition and regulation of profiling and targeted advertising, the legal framework, data subjects’ rights (including the right to access and delete information), consent for data processing and the requirements for such consent, accountability and sanctions, data breach notifications, cross-border data transfers, and the presence of a supervisory authority. An important component of the methodology was the analysis of judicial practice in Kazakhstan and the European Union. This section of the study examines Kazakhstani and European cases related to profiling and targeted advertising: a woman questioned the legality of fingerprint access control at work (Open Dialog, 2022b), a person asked if written consent is needed for workplace video surveillance (Open Dialog, 2022a), a company was questioned about recording customer service interactions and need for consent (Open Dialog, 2021a), a person raised concerns about personal data in vaccination QR codes (Open Dialog, 2021b), *Meta (Facebook) v. German Anti-trust Authorities* (EU’s Top Court..., 2023), *CNIL v. Google* (The CNIL’s Restricted..., 2019), *ICO v. British Airways* (Prinsley *et al.*, 2020), the *Case Against IAB Europe* (The BE DPA..., 2022), the *Oracle and Salesforce lawsuits* (Privacy Collective, 2020), and the *Luxembourg Data Protection Authority v. Amazon* (Luxembourg DPA Fines..., 2021).

To analyse the practical implementation of the legal regulation of profiling and targeted advertising in Kazakhstan, monitoring was conducted between January and March 2024 on three popular online platforms: News Portal Kaspi – the largest platform in Kazakhstan in the fields of e-commerce and online banking, which actively utilises users’ personal data to generate personalised offers and advertisements; Tengrinews – a popular news portal widely used for obtaining information and advertisements, including those with elements of targeting, making it relevant for exploring profiling in the news sector; and Platform for Selling and Buying Real Estate Krisha (2024), which actively employs user profiling to provide advertising offers based on their

search queries. The monitoring was based on criteria such as the transparency of privacy policies, the clarity of user consent for data processing, the extent of user control over personal data, and the implementation of targeted advertising practices. The observation focused on the use of cookies, the methods of obtaining consent for data processing, and how the platforms manage user data for advertising purposes. The choice of these platforms was justified by their popularity and wide application in Kazakhstan. Each platform represents a unique example of the use of personal data in different sectors – e-commerce, news resources, and real estate – which provides an opportunity to comprehensively review the practice of profiling and targeted advertising.

Results

Legal aspects of regulating profiling and targeted advertising. Targeted advertising and profiling have become integral elements of modern marketing strategies. Targeted advertising is the process through which advertising materials are directed at carefully selected audience segments. Such segments are formed based on user data, including demographic information, search history, behavioural patterns, interests, and other digital traces they leave online. Profiling, in this context, is a key tool used for analysing and interpreting these data. It enables the creation of detailed digital profiles of users, allowing advertisers to more accurately predict their preferences and needs. This not only enhances the relevance of advertising messages but also increases the effectiveness of marketing campaigns.

However, the widespread adoption of profiling and targeted advertising raises several ethical and legal concerns. Chief among these is the issue of data privacy. Users may be unaware of the extent and type of data being collected about them, as well as how this data will be used in the future (Mentukh & Shevchuk, 2023). This leads to concerns about potential violations of privacy rights and the misuse of personal information. Legislative acts, such as Regulation of the of the European Parliament and of the Council No. 2016/679 “On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive No. 95/46/EC (General Data Protection Regulation)” (2016), set forth clear requirements for the processing, storage, and collection of personal information. Advertising companies are obliged to comply with these rules to safeguard user rights and ensure transparency in their actions.

Regulation of the European Parliament and of the Council No. 2016/679 (2016) established rules for the protection of personal data and strengthened control over its processing and transfer, both within the EU and beyond, where such data concerns Union citizens. The main provisions of the GDPR regulate principles of data interaction, define the rights of data subjects, outline measures of responsibility and penalties, and establish rules for cross-border data transfers. The GDPR mandates the following principles: legality, transparency, and fairness in data processing (Article 5(1)(a)). Data must be collected with a clearly defined purpose, and further processing that does not align with the initially stated objectives is prohibited (the principle of purpose limitation) (Article 5(1)(b)). Data processing must be minimised, meaning only the information genuinely required to achieve a specific, defined task may be requested (the principle of data minimisation) (Article 5(1)(c)). Data must be stored only for

as long as is necessary to achieve the purposes of its processing (the principle of storage limitation) (Article 5(1)(e)).

Furthermore, the GDPR sets requirements for protecting data against unlawful processing and unauthorised access, as well as accidental loss, damage, or destruction (the principle of integrity and confidentiality) (Article 5(1)(f)). An important aspect is the requirement for accuracy: data must be updated as necessary and must reflect reality (the principle of accuracy) (Article 5(1)(d)). The rights of data subjects include access to their information, enabling them to understand what data is being collected and how it is being used; the ability to correct inaccuracies in the information; the possibility to delete data (the so-called “right to be forgotten”) if it is no longer required (Article 17); the ability to restrict processing (Article 18); and the right to obtain data in a convenient format for transfer to another controller (Article 20). Users may also object to the transfer of their data in certain cases, such as for direct marketing purposes (Article 21).

The GDPR provides for strict measures of responsibility for violations of its provisions, with fines of up to 4% of the company’s annual turnover or EUR 20 million, whichever is higher (Article 83). The regulation also requires companies to appoint Data Protection Officers (DPOs) when handling personal information is a core activity and involves monitoring a wide range of data subjects (Article 37). Moreover, the GDPR establishes strict rules for the transfer of information outside the EU. Transfers are permitted only to countries with an adequate level of data protection or based on legal grounds such as standard contractual clauses (Article 46). The GDPR has significantly strengthened citizens’ rights to control their personal data and imposed strict obligations on companies to ensure this protection.

As of mid-2024, the GDPR is implemented across all 27 EU Member States, including countries such as Germany, France, Italy, Spain, and others, as well as in EEA countries such as Norway, Iceland, and Liechtenstein. Following the United Kingdom’s exit from the EU (Brexit), the UK adopted its own version of the GDPR – UK GDPR – which is nearly identical to the European regulation but applies exclusively within the United Kingdom (Luisi, 2022). The GDPR also applies to companies and organisations located outside the EU or EEA that offer goods and services to EU citizens or monitor their online activities (Jones & Kaminski, 2020). This means that any company handling the data of EU citizens must comply with the GDPR, regardless of its geographic location.

A different situation is observed in countries outside the EU’s legal jurisdiction that aspire to adopt its advanced and progressive practices. For instance, Kazakhstan has not fully implemented the GDPR but has been gradually adapting its standards since 2019. From August 2019, Kazakhstan began preparing a draft law introducing amendments to the country’s data protection regime based on the GDPR and the establishment of a specialised agency dedicated to personal data protection (Khamidullina, 2019). The draft, titled Law of the Republic of Kazakhstan No. 347-6 ZRC “On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan Regarding Regulation of Digital Technologies” (2020), as of August 2019, proposed amendments and additions to a significant number of laws and codes of Kazakhstan, including the Law on Data Protection. The draft referenced the GDPR as an internationally studied practice and included provisions for creating an authorised state body to handle personal data issues.

The following changes to personal data regulations were adopted. Kazakhstani companies were required to notify the Law of the Republic of Kazakhstan No. 44-VIII “On Amending Certain Legislative Acts of the Republic of Kazakhstan on Information Security, Informatisation and Digital Assets” (2023) (a requirement similar to that in the GDPR). This meant that Kazakhstani companies are required to notify relevant authorities about certain activities related to information security, data processing, and digital assets. This requirement is similar to the GDPR, which mandates companies to inform data protection authorities and affected individuals in the event of data breaches or violations. Next, the “localisation rule” was clarified by specifying that personal data of Kazakhstani citizens must be stored and processed within the territory of Kazakhstan. And finally, the duties of the State Technical Service of the National Security Committee were expanded to include inspections of personal data security (companies were obliged to grant the Service access for such inspections). Furthermore, from July 2020, companies were mandated to establish a role analogous to the Data Protection Officer (DPO), introduced in the EU in 2018, requiring the appointment of an individual responsible for managing personal data (Kazakhstan Strengthens Personal..., 2021). These innovations were approved under the Law of the Republic of Kazakhstan No. 399-4 “On Introducing Amendments and Additions to Some Legislative Acts of the Republic of Kazakhstan on the Issues of Restoration of Economic Growth” (2021). Despite the relatively small fines in both cases (100 monthly calculation indices, equivalent to approximately USD 630), these decisions demonstrated that the Ministry was prepared to take tangible measures to protect personal information.

As of mid-2024, the regulation of targeted advertising in Kazakhstan is implemented through several key laws and regulations. The Law of the Republic of Kazakhstan No. 508-2 (2003) regulates all types of advertising, including online advertising, within Kazakhstan. It sets general rules for advertising, requirements for its accuracy, and prohibits certain types of advertising (e.g., unfair or misleading advertising). The law also defines liability for violating advertising legislation. The Law of the Republic of Kazakhstan No. 94-5 (2013) governs the processing of personal information, including data used for targeted advertising. It stipulates that personal data can only be processed with the owner’s consent and establishes rules for its protection and handling. Within the framework of this law, requirements are set for database operators who collect and process personal data, including requirements for their protection and the maintenance of confidentiality. The Law of the Republic of Kazakhstan No. 18-8 (2023) regulates the activities of online platforms where online advertising, including targeted advertising, is placed. The law defines the obligations of platform owners to protect user data, requires transparency in the functioning of platforms, and limits the dissemination of illegal content. A key aspect of this regulation is the governance of recommendation systems and the use of profiling for targeted advertising. These laws form the legal foundation for the regulation of targeted advertising in Kazakhstan, ensuring the protection of user rights and establishing liability for advertisers and online platform operators. However, there are still many areas where the legislation of Kazakhstan lags behind European standards.

Comparison of key provisions of Kazakhstan and the EU legislation regulating profiling and targeted advertising.

The legislation of Kazakhstan concerning profiling primarily relies on the provisions of the Law of the Republic of Kazakhstan No. 94-5 (2013) and the Law of the Republic of Kazakhstan No. 18-8 (2023). In Kazakhstan, profiling involves the use of algorithms that evaluate the interests and preferences of users to generate individualised advertising. Data operators must obtain users' consent to process their personal information, including profiling, which is used for targeted advertising. In Europe, profiling is regulated by Article 22 of the GDPR, which defines it as an automated process involving personal data to analyse various aspects of an individual's personality, such as financial status, health, preferences, and other parameters. Under GDPR requirements, data processing for profiling is only permitted if there is "explicit consent" from the data subject (Article 6(1) (a)). Unlike the legislation of Kazakhstan, where profiling is predominantly used for targeted advertising, the GDPR introduces stricter restrictions. Specifically, it prohibits automated decisions that may affect citizens' rights and freedoms if made without human involvement (Article 22).

The legislation of Kazakhstan also regulates targeted advertising through the Law of the Republic of Kazakhstan No. 18-8 (2023). Targeted advertising is defined as advertising directed at specific target groups based on profiling. The law requires online platforms to provide users with the option to opt-out of targeted advertising and ensure full transparency regarding the profiling methods used. In the EU, targeted advertising is regulated by both the GDPR and the Directive of the European Parliament and of the Council No. 2002/58/EC (2002). As in Kazakhstan, the GDPR mandates consent for the processing of data used for targeting. However, the Directive introduces additional requirements related to the use of cookies and other tracking tools that monitor users' online behaviour. The Directive requires websites to obtain active and informed consent from users for the use of cookies if they collect personal data, which is often the basis for profiling and targeted advertising. Notably, in the EU, ePrivacy is often applied in conjunction with the GDPR (Yakymenko, 2023). This way it provides stricter oversight of targeted advertising processes because it imposes additional requirements on the use of cookies and tracking technologies for targeted advertising.

According to the Law of the Republic of Kazakhstan No. 94-5 "On Personal Data and Their Protection" (2013), simple consent from users is required to process information for profiling and targeted advertising. Users must be fully informed about the purpose of collecting such information, how it is used, and be aware that they have the right to withdraw consent for processing this data at any time. However, the law in Kazakhstan does not specify that consent must be explicit, voluntary, and unambiguous, as is required under European regulations. The GDPR requires explicit consent but also introduces additional requirements for informing users. In particular, consent must be given voluntarily, consciously, clearly, and unambiguously. This means that the user must take a clear, affirmative action to indicate consent, and the consent must be separate from other agreements or terms of service. Users must be thoroughly informed about the purpose of collecting such information, how it is used, and be aware of all their rights, including the right to withdraw consent for processing such data at any time

(Shtovba, 2024). The GDPR insists that the consent process be separate from other agreements and that the procedure for withdrawing consent should be simple and accessible. This adds a layer of clarity and user control that goes beyond the simpler consent requirements in Kazakhstan's legislation.

The Article 147 of the Penal Code of the Republic of Kazakhstan (2014) also provides for administrative fines for violations related to profiling and targeted advertising, but the amounts of these penalties and the procedures for their application are less strict compared to European standards (GDPR, Article 83). Companies can be fined for improper use of personal data or for insufficient measures to protect it. The GDPR clearly specifies fines for non-compliance, including violations related to profiling and targeted advertising. The fines are determined based on the maximum amount, which may be either 4% of annual turnover or EUR 20 million. This makes the GDPR one of the strictest legal frameworks for data protection.

Meanwhile, some authors such as Yerbolatov (2022), Iskakova and Kadyrzhanova (2022) note that there is a difference in the rights of data subjects. While in Europe, data subjects have broad rights, including access to their data (GDPR, Article 15), the right to correct inaccuracies (GDPR, Article 16) and portability (GDPR, Article 20), and the right to erasure (GDPR, Article 17), in Kazakhstan, the rights of subjects are more limited. Individuals have some ability to control their personal information, such as the right to erasure (Article 19) (Law of the Republic..., 2013), but these rights are not as extensive or as easily enforceable as under the GDPR (Yerbolatov, 2022). In addition, although Kazakhstan has a supervisory authority, its powers and independence may be more limited compared to similar authorities in GDPR-compliant countries. There are also requirements for data breach notifications, but the timelines and conditions are different. The GDPR requires companies to notify authorities within 72 hours of a data breach (Article 33), while in Kazakhstan it should be done during one business day (Law of the Republic..., 2013) (Iskakova and Kadyrzhanova, 2022). Thus, the legislation of Kazakhstan in the area of profiling and targeted advertising is largely similar to European legislation, particularly in terms of consent and transparency requirements – Law of the Republic of Kazakhstan No. 94-5 (2013) and Article 6 of the GDPR. However, European regulation, represented by the GDPR (2016) and the ePrivacy Directive (Directive of the European..., 2002), is more detailed and imposes stricter restrictions and liabilities on companies engaged in profiling and targeted advertising. The norms of Kazakhstan aim to achieve similar goals but with consideration of national law enforcement practices and legal culture.

Analysis of judicial practice. There are numerous precedents involving highly contentious issues faced by law enforcement practices in relation to personal information protection. For instance, a case can be cited where a woman approached the Minister of Labour and Social Protection questioning the legality of an employer introducing an access control system based on fingerprint identification (Open Dialog, 2022b). She argued that fingerprints are classified as personal data. The Ministry responded by highlighting the mandatory compliance with the provisions of the Law on Personal Data, including the requirement to obtain employee consent (Open Dialog, 2022b). The response also needed to clarify that fingerprints are classified as biometric personal information and that the collection of such data may only

be conducted by authorised bodies (Law of the Republic of Kazakhstan No. 94-5, 2013). However, even in cases where the employer's activity aligns with legal requirements, the collection of fingerprint data for employee identification may violate the principle that only personal data necessary and sufficient for achieving specific purposes should be collected and processed.

Questions about the legality of video surveillance and recording in the context of labour and commercial relations between citizens and businesses have also been raised in various appeals to ministries (Akhmetova, 2023). For example, a person inquired whether employers are required to obtain written consent from employees for video surveillance at the workplace, citing potential violations under Article 147 of the Criminal Code of Kazakhstan (violating privacy and data protection laws) (Open Dialog, 2022a). In another case, a commercial organization was questioned about its practice of video and audio recording customer service interactions, specifically whether this constitutes personal data processing and if consent is required (Open Dialog, 2021a). In a different case, a person raised concerns about the disclosure of their personal data (including full name and ID number) when presenting vaccination QR codes, questioning whether this constitutes a violation of personal data protection (Open Dialog, 2021b). In responses from state authorities, it is generally noted that the collection and processing of personal information must comply with legislative requirements, including mandatory notification and obtaining consent for video surveillance (Law of the Republic of Kazakhstan No. 94-5, 2013). These responses suggest the permissibility of collecting and processing data through video surveillance, provided that facial imagery is necessary and sufficient to fulfil the objectives of the employer or business entity. Nevertheless, state authorities must emphasise more clearly that the data collected should be limited to information critically essential for processing purposes. As mentioned earlier, ensuring high-quality awareness for both citizens and businesses promotes the development of legal culture and contributes to the effective implementation of laws in the country. Numerous such precedents exist, particularly at local levels. Alignment with the GDPR and EU practices would help avoid such cases by establishing clear, standardized procedures for obtaining explicit consent, ensuring transparency in data collection, and enhancing accountability in personal data processing. To avoid misunderstandings over privacy rights, the GDPR requires comprehensive consent standards, such as unambiguous notifications and the ability to revoke consent. In order to guarantee that companies handle personal data with the highest care and responsibility, it also enforces stringent safeguards for biometric data, video surveillance, and the use of personal identifiers like QR codes (Zaki *et al.*, 2021). This alignment would strengthen the foundation for safeguarding people's privacy, lower legal risks, and increase consumer trust.

By comparison, in the case of Meta (Facebook) versus German Antitrust Authorities (EU's Top Court..., 2023), where the German antitrust authority accused Meta of abusing its dominant position by linking data usage with access to platforms (Facebook, Instagram, and WhatsApp), the Court of Justice of the European Union (CJEU) ruled that Meta violated the GDPR by using user data for targeted advertising without explicit consent. This limited the company's ability to utilise data for advertising in Germany and

led to significant financial losses. The decision paved the way for similar cases across the EU (EU's Top Court...). In 2019, the French CNIL Commission fined Google 50 million euros for violating GDPR. The main issue was the lack of transparency and the absence of informed consent from users regarding the collection of data for advertising. Google did not provide sufficient information on how it used data for targeting and did not obtain explicit permission for this (The CNIL's Restricted). In 2020, the UK's Information Commissioner's Office (ICO) imposed a fine of 20 million pounds on British Airways for a data breach affecting 400,000 users (Prinsley *et al.*, 2020).

Special mention should also be made of judicial decisions that can be considered exemplary in terms of fairness and a civilised approach, which should be adopted by the judiciary of Kazakhstan. In the "Case against IAB Europe" (The BE DPA..., 2022), the Belgian data protection authority ruled against IAB Europe, stating that their system for obtaining consent for targeted advertising (TCF) violated GDPR. The court required the company to revise its procedures and imposed a fine of EUR 250,000. However, the important point was that the court gave the company the opportunity to correct the deficiencies in its system, maintaining a balance between data protection and advertising interests (The BE DPA..., 2022). In the Netherlands, Oracle and Salesforce companies (Privacy Collective, 2020) were subject to legal proceedings for using user data for targeted advertising without proper consent. Unlike other cases, the court recommended that the company reconsider its methods and give users more control over their data. This decision demonstrated a civilised approach, where companies were given the opportunity to adapt to new standards without imposing significant fines. Also noteworthy is the precedent with Amazon (2021). The Luxembourg data protection authority fined Amazon a record 746 EUR million for violating GDPR (Luxembourg DPA Fines..., 2021). Nevertheless, when making the decision, the court emphasised that Amazon could improve its data collection processes and provide greater transparency to users regarding the use of their data for targeting. This decision became an example of courts striving to achieve a fair balance between business interests and user rights protection (Top Websites Ranking, 2024). These cases highlight a broader trend in judicial practice, where courts seek to balance regulatory enforcement with the opportunity for companies to rectify compliance issues, promoting both legal accountability and a fair business environment.

Specifics of targeted advertising and profiling on online platforms in Kazakhstan. To analyse the use of targeted advertising and profiling on online platforms in Kazakhstan, with a focus on legal aspects, popular Kazakhstani online platforms (e-commerce sites, social networks, news portals, etc.) were selected. These platforms actively use targeted advertising (notable ad campaigns, banners, pop-up messages) containing information about personal data processing policies and user consent. According to the Top Websites Ranking (2024), as of mid-2024, platforms such as the E-Commerce and Online Banking Platform Kaspi (2024), the popular news portal Tengrinews (2024), and the Platform for Selling and Buying Real Estate Krisha (2024) are highly popular among internet users in Kazakhstan.

On the Kaspi website, there is a privacy policy that contains information on how the company collects, processes, and protects users' personal data (Code of Ethics and

Business..., 2025). This policy outlines the key provisions regarding the storage and processing of data and its use for commercial purposes. The Kaspi privacy policy mentions the use of user information for personalised advertising and marketing. It also emphasises that the company is obliged to comply with the requirements of the legislation of Kazakhstan, particularly the Law of the Republic of Kazakhstan No. 94-5 (2013). Despite this, the policy may not detail how the explicit consent of the user for targeted advertising is collected, which could become a problematic point in terms of meeting strict requirements similar to the GDPR. Kaspi uses cookies, but the privacy policy does not always clearly state whether user consent is requested for their use, as required by European legislation such as the GDPR (Article 6(1)(a)). In Europe, users must be able to give explicit consent for the use of cookies for targeted advertising purposes, and they must also have the ability to easily opt-out of this. Users of the platform can manage some aspects of their data, for example, through account settings or when interacting with support. Nevertheless, the ability to fully manage personal data, including its deletion or restriction of use, may be limited and does not meet the standards set in the EU, such as the right to be forgotten (GDPR, Article 17) and the right to data portability (GDPR, Article 20). If Kaspi were operating within Europe, it could face a number of legal issues. The use of personal data for advertising without obtaining explicit user consent would violate GDPR rules (Article 6(1)(a)). Moreover, failing to inform users about how their data is processed could lead to fines. The lack of full control over their information, including the right to deletion (Article 17), would also be considered a violation of European laws. As a result, Kaspi would have to significantly revise its policy and procedures regarding data to comply with the strict GDPR standards required to operate in the EU.

The Tengrinews website contains a privacy policy and terms of use for data (Privacy Policy, 2025). These documents describe how the platform processes users' personal data, how it may be used, and what measures are taken to protect it. Specifically, information may be collected to improve the services and to display ads tailored to users' interests. The privacy policy provides general information on the collection and use of data for advertising but may not meet all the strict requirements of European laws such as GDPR. For example, obtaining user consent for data processing and targeted advertising is not always detailed, which may be problematic from the perspective of European standards (GDPR, Article 6(1)(a)). It is also not clearly stated how users' data is processed in accordance with the data protection norms of Kazakhstan. The website uses cookies to track user activity and improve advertising, but consent for the use of these files is not always explicitly requested, as required by European standards (ePrivacy Directive, Article 5(3)). European laws such as GDPR require explicit user consent for the use of cookies for targeted advertising, which may not be complied with in this case (GDPR, Article 6(1)(a)). However, Tengrinews does provide limited data management options. Users can manage profile settings, but more detailed rights (such as the right to deletion or data portability) provided by the GDPR may be absent (Article 17; Article 20). If Tengrinews were operating in Europe, the website would face a number of legal issues. Particularly notable is the lack of explicit consent for the use of cookies and data collection for

advertising, which violates the GDPR norms (Article 6(1)(a)). Furthermore, the absence of more detailed mechanisms for managing users' personal data, such as the right to deletion or data portability, could lead to sanctions (Article 17; Article 20). The lack of transparency in the privacy policy and terms of use may also raise concerns from regulators in Europe (Article 13).

The Krisha website presents a privacy policy and personal data processing terms. It describes the rules under which user data is collected and processed, including information about activities on the site, browsing history, IP addresses, device data, and advertising identifiers. The site operates within the framework of the legislation of Kazakhstan, but details about compliance with international standards such as the GDPR are absent. The Krisha policy allows for the processing of data to provide advertising and marketing services, facilitating the use of targeted advertising. However, compared to European standards such as the GDPR, it is not entirely clear how explicit user consent for data processing for these purposes is implemented (Article 6(1)(a)). The policy also lacks detailed information about users' rights to access their data or delete it, which could be an issue in the European context (Article 17; Article 20). The site uses cookies to improve functionality, but the process for obtaining explicit consent for the use of these files for advertising purposes is not as clearly stated as required by European standards (Article 6(1)(a)). In particular, users may not be fully informed about what data is collected through cookies and how it is used for advertising, which violates GDPR rules (Article 13). Krisha also provides limited options for data management. Users can update profile information and manage ads, but rights to delete data or restrict its use are not described as thoroughly as required by European rules (Article 17; Article 20). This could create issues for users if the site were operating within the EU. If the Krisha portal were operating in Europe, it could face problems related to the lack of explicit consent for data processing for targeted advertising and the use of cookies (Article 6(1)(a)). The lack of transparency in the privacy policy and the limited options for users to manage their data could lead to GDPR violations (Article 13). This could result in both fines and restrictions on access to the EU market.

An analysis of the three main online platforms in Kazakhstan showed that while fundamental data protection measures, such as privacy policies and the use of cookies, are in place, the overall level of personal data protection does not meet the stringent standards set by the GDPR in the EU. The key issues include a lack of transparency, the absence of explicit user consent for the use of personal data in targeted advertising and cookies, and limited options for users to manage their data. Although there are laws in Kazakhstan, such as the Law of the Republic of Kazakhstan No. 94-5 (2013), the current implementation of these protective measures does not align with European standards, which could result in legal challenges if these platforms were to operate in the EU.

Recommendations for improving legislation in line with international standards. In terms of legal risks, the absence of explicit user consent for targeted advertising violates Article 6(1)(a) of the GDPR, which requires that personal data processing for advertising purposes be based on explicit consent. This could potentially lead to fines and restrictions on the use of personal information, as outlined in

Article 83 of the GDPR, which specifies fines for non-compliance. Furthermore, users are often not fully informed about how their data is collected and processed, creating a gap in transparency and constituting a breach of Article 13 of the GDPR. This Article mandates that users be informed about how their data will be used and processed at the time of collection, ensuring transparency in data practices. Another issue is the limited ability of users to manage their data, including the right to request deletion or restrict data processing, which further increases legal risks under the GDPR. Specifically, Article 17 of the GDPR guarantees the right to deletion of personal data, also known as the “right to be forgotten”, and Article 20 of the GDPR grants users the right to receive their data in a commonly used, machine-readable format and transfer it to another controller. These articles aimed at ensuring user control over their personal information.

The situation could be improved by meeting several requirements, which are already mandated by the existing and actively enforced laws of Kazakhstan. For example, platforms should implement mechanisms for obtaining explicit user consent for the use of data for advertising and cookies, in accordance with Article 6(1)(a) of the GDPR, which requires explicit, informed consent. Companies should provide more detailed and accessible information about the data collected, how it is used, and how users can manage their data. This would align with Article 13 and Article 14 of the GDPR, which mandate clear, transparent information for users regarding the processing of their data. Privacy policies should be written in a clear format and updated regularly, as required by Article 12 of the GDPR. In addition, platforms should enable users to exercise full control over their data, including the right to data deletion (right to be forgotten) and the right to data portability, which are key provisions of Articles 17 and 20 of the GDPR. To enhance competitiveness in international markets and improve user trust, Kazakhstani platforms should strive for GDPR compliance, which would not only improve data protection but also provide access to the European market without the risk of sanctions. This alignment with the GDPR would be critical for expanding their user base in the EU and ensuring legal compliance, as outlined in Article 45 of the GDPR.

Some other countries have unified their data protection laws with the GDPR to resolve discrepancies akin to those found in Kazakhstan’s rules. For example, the Brazilian General Data Protection Law (2018) (LGPD). The GDPR serves as an inspiration for the LGPD, which sets forth extensive data protection guidelines. It guarantees transparency in data collection and use, requires organisations to have express consent before processing data, and gives people rights including data access, correction, deletion, and portability. These clauses support user confidence and ease cross-border data transfers by being in line with GDPR rules. In order to improve data protection measures, Japan’s Act No. 57 on the Protection of Personal Information (2003) was updated in 2020. Stricter rules on data processing were brought about by the changes, which included specifications for getting consent, guaranteeing data correctness, and putting security measures in place. These modifications improve user confidence and facilitate more seamless data exchanges with EU nations by bringing Japan’s data protection system closer to GDPR standards. These nations have improved their data governance systems and increased their competitiveness in global markets by enacting GDPR-aligned data protection

regulations. Following strict data protection guidelines makes cross-border data transfers easier, lowers the possibility of legal issues, and increases user and business partner trust. Adhering to GDPR guidelines would also improve user confidence, make it easier for Kazakhstani platforms to access the European market, and reduce the possibility of sanctions, all of which would increase their global competitiveness. Nevertheless, the protection, processing, and use of personal data in Kazakhstan, particularly in the context of targeting and profiling, fail to address the growing influence of artificial intelligence tools utilised in these processes. This omission appears logical, as the use of such tools is often costly and, therefore, not as widespread outside America and the EU, including in Kazakhstan.

An interesting solution could be the implementation of blockchain as a decentralised digital system for data storage and transmission, which would make data collection and processing more transparent and secure. If internet resources in Kazakhstan employed blockchain to store user data (for example, information about transactions or preferences), this could ensure a high level of personal data protection. In this regard, M. Poelman and S. Iqbal (2021) noted potential challenges regarding rights such as the “right to be forgotten”, since data stored on the blockchain cannot be deleted. However, this issue could potentially be circumvented by directing blockchain towards the creation of so-called “trusted advertising”. In this case, user data would be stored on the blockchain and used for targeted advertising, but access to this data would be controlled and transparent for the users themselves, thereby enhancing the level of protection of their personal information. The relevance of blockchain technology to Kazakhstan and its ability to address numerous problems related to personal data protection was also highlighted by Y. Akhmetbek and D. Špaček (2021). Furthermore, it is worth noting the study by H. Kocharyan *et al.* (2021), which questions the effectiveness of the right to be forgotten in terms of privacy protection. The authors conclude that although this right is important for safeguarding confidentiality, its implementation faces significant challenges and is not always effective in guaranteeing the complete deletion of personal information. In this context, when comparing the uncertain possibility of deleting data with a technology that enhances the security of its storage and use, the choice becomes obvious, at least from the perspective of the legal aspects of protecting the rights of internet users and consumers of advertising content.

Discussion

The legal framework for profiling and targeted advertising in Kazakhstan reflects an effort to align with legislation, such as the Law of the Republic of Kazakhstan No. 94-5 (2013). However, the level of data protection and transparency regarding targeted advertising falls short of European standards, particularly the requirements of the GDPR. The main issues include the absence of explicit consent for the use of data, insufficient transparency concerning data processing, and limited options for users to manage their personal data. This creates legal risks for platforms in Kazakhstan, should they operate in Europe.

The study noted numerous challenges that Kazakhstan has already encountered on its path towards implementing new standards, including financial obstacles, as the introduction of mechanisms that fully ensure compliance with all

legal aspects related to the security and use of personal data for targeted advertising and profiling requires significant financial investments from companies in Kazakhstan. The fact that the implementation of the GDPR also affects market competition, including both large and small companies, as well as their ability to protect themselves within the legal framework, was also highlighted by M.S. Gal and O. Aviv (2020). The authors highlighted the GDPR's restrictions on using personal data for such purposes without explicit user consent and discussed the substantial impact of these restrictions on the digital advertising market and competition among companies that rely on such methods, which often prompts attempts to circumvent the legal regulatory framework.

The study also highlighted the challenges faced by companies and organisations in Kazakhstan when attempting to implement the GDPR and other European standards regulating advertising activities. For instance, the most common legal violations in Kazakhstan are insufficient user notification, failure to meet consent requirements, and improper data management. These issues are characteristic of other countries as well, as evidenced by the studies of M. Kive and J. Grasis (2020) and W. Presthus and K.F. Sønslie (2021). In this context, it is also worth mentioning the study by A. Wodi (2023), in which the author analysed the outcomes of the GDPR five years after its adoption, examined the future of personal data protection, assessed the effectiveness of the GDPR in ensuring data security, identified unresolved challenges, and explored how the regulation may evolve in the future. To the aforementioned issues, A. Wodi (2023) also added the discrepancies in the enforcement of laws related to targeting and profiling in advertising which are influenced by aspects and nuances of the extraterritorial application of the GDPR. This is particularly relevant for countries in Central Asia, including Kazakhstan. Researcher emphasised that the effectiveness of regulating the advertising sphere cannot be assessed in isolation from the legal frameworks of each country, within which these European legislative norms are implemented. The author also considered the prospects for legal regulation of advertising, a field that is expected to become increasingly complex with the advancement of technologies such as artificial intelligence, blockchain, and big data.

Among other conclusions, the authors argued that the legal maturity of countries plays the most critical role in determining the choice of approaches and tools for regulating the advertising sphere and protecting the rights of internet users. This also affects the actual, rather than formal, implementation of the adopted regulations. A. Prasad and D.R. Perez (2020) concluded that while the GDPR had positive effects in data protection, it may also harm innovation and the development of the digital business sector, particularly in advertising and data analytics. This, too, must be considered when developing legal mechanisms for regulating this sphere, as the legislation of a country should foster the growth of local businesses rather than place them in a position where they cannot effectively compete with financially stronger and legally better-protected international giants.

The conducted study also identified shortcomings in the practical implementation of the legislation of Kazakhstan in the regulation of advertising and the use of users' data for advertising purposes, based on the analysis of several popular Kazakhstani internet platforms. A study by M. Kretschmer *et al.* (2021) also noted that the use of cookie banners

and privacy policies on websites often deviates in practice from the norms and legal practices adopted under the specific legislation of a country. The authors discussed issues related to the implementation of GDPR requirements, such as the complexity of privacy policy wording and its potential impact on user experience, which are also characteristic of Kazakhstan, as confirmed by this study. Moreover, the studies by L. Porcelli *et al.* (2024), and C. Santos *et al.* (2021) highlight the improper application of certain legal norms (including penalties for violations) in cases (countries, conditions) where organisations or enterprises are objectively unable to meet all the technical requirements necessary to comply with the legal conditions for handling users' personal data. This is particularly relevant to Kazakhstan during the period from 2020 to 2024.

The technical feasibility of complying with legal norms related to the collection and use of personal data, including in the context of advertising activities (particularly targeting and profiling), was also addressed by A. Kajcsa and L. Dogaru (2022). Among other issues, they highlighted a problem specific to Kazakhstan, which was also identified in this study: namely that data deletion, especially from complex AI systems, can be technically challenging and may not align with the immutability principles of certain systems, which should be considered in the legal field (but is absent in the regulations governing this area in Kazakhstan). In their paper, K. Wiedemann (2022) also addressed the regulation of profiling in the context of automated decision-making processes, including those involving the use of personal data for targeted advertising. The author emphasised that while the GDPR contains strict rules for automated decision-making, companies may face difficulties in complying with them, particularly in profiling for advertising purposes. However, they remarked that technical measures can assist in ensuring compliance with GDPR requirements, especially regarding transparency and obtaining consent, which should also be noted by Kazakhstan.

The study repeatedly mentioned, in various contexts, issues related to ensuring the protection of privacy rights in Kazakhstan, particularly in areas such as advertising, targeting, and profiling. The presented findings highlighted that the situation in Kazakhstan differs from European practices, as evidenced by the study of R.N. Zaeem and K.S. Barber (2020), which examined the impact of the GDPR on the privacy policies of enterprises and organisations. Their study identified key improvements in European and American approaches, particularly through the introduction of tools that provide users with greater control over their data, including the right to access, modify, and delete personal information. These improvements directly address some of the most pressing issues observed in Kazakhstan, and the authors also emphasised the importance of improving the legal framework governing advertising and personal data management, offering several solutions that Kazakhstan could adopt and implement within its legal system. In the same context, the paper by M. Bak *et al.* (2022) can also be considered, focusing on the legal regulation of the right to privacy and its enforcement concerning medical data, which may also be used for targeted advertising of specific medical devices and medications. Public display of such information could not only violate a user's right to privacy but also breach medical confidentiality, potentially causing reputational damage or psychological harm in certain cases.

This study also underscored that the supervisory authority in Kazakhstan not only has limited powers and independence compared to similar bodies in GDPR-compliant countries but also lacks adequate tools for monitoring and regulation specifically tailored to the realities of Kazakhstan. This problem is also noted by S. Amanzholova *et al.* (2021), who developed a tool that allows for the automated verification of websites' compliance with key GDPR aspects, such as data protection, transparency, and user consent collection and usage. This system needs to be tested in practice and integrated into the legal regulation mechanism of the advertising sector before the state can fully implement a legal framework for enforcement, monitoring, and the imposition of legal sanctions for non-compliance. Moreover, the mechanism proposed by the authors could be applied not only to the advertising sector but also to combating cyber corruption. In the study by S. Gulyamov and S. Raimberdiyev (2023), it was noted that Kazakhstan's inability to fully ensure the protection of personal data leads to cyber corruption and other cybercrimes involving the violation of user rights, highlighting the importance of implementing not only effective legal but also technical measures to regulate this area. Furthermore, Kazakhstan should also consider the need to adapt to other aspects of technological development, such as Regulation of the European Parliament and of the Council No. 2024/1689 (2024), mentioned in the study by C. Lawson-Hetchely (2022). This regulation will impose additional requirements on companies already operating under GDPR, significantly increasing the demands on legal regulation mechanisms for the use of artificial intelligence, particularly concerning the collection and processing of personal data necessary for targeting and profiling.

Thus, the problems faced by Kazakhstan in regulating profiling and targeted advertising are not unique and are largely similar to the issues experienced by other countries, particularly those that implemented international GDPR standards earlier and more comprehensively. This indicates that Kazakhstan is moving in the right direction, considering its current stage of legal and technological development. Moreover, this provides the country with an opportunity to learn from the mistakes of others and adopt proven practices from countries that have already succeeded in these areas.

Conclusions

The study identified key differences between regulation of profiling and targeted advertising in Kazakhstan and the European Union, particularly in the context of applying GDPR standards. The legislation of Kazakhstan in the area of

personal data contains basic elements of data protection, such as requirements for obtaining user consent and privacy policies. However, the analysis of three major online platforms (Kaspi, Tengrinews, Krisha) revealed that local data protection norms have gaps compared to European standards.

The comparative analysis of the legislation of Kazakhstan and European norms (GDPR) demonstrated substantial differences in approaches to personal data protection. The main distinction is the mandatory obtaining of explicit user consent in the EU for data collection and processing, whereas, in Kazakhstan, this process may be less detailed and does not require such a high degree of transparency. European legislation also provides a broader set of rights for data subjects, including the right to data portability and deletion, which is insufficiently reflected in the laws of Kazakhstan. Furthermore, the EU has strict requirements for notifying users about data security breaches, while in Kazakhstan, this aspect may not be sufficiently developed. These differences create the need for modernising the legislation of Kazakhstan, especially in light of its aspirations to integrate with international markets and comply with global data protection standards.

Notably, Kazakhstani online platforms face a number of problems in the processing and protection of personal information. Users are not always able to give explicit consent for the use of data for targeted advertising. Privacy policies are often insufficiently transparent and understandable, which means that users are poorly informed about how their data is used. These issues are particularly important in the context of GDPR compliance, which requires strict adherence to transparency and consent rules. In addition, the analysis showed that platforms provide limited opportunities for managing personal data. Users can update their profile information but do not have full control over their data, including the right to delete or transfer it. This contradicts European norms, which grant EU citizens broader rights regarding their data.

Future research could focus on a detailed comparative analysis of practices on other key platforms and industries in Kazakhstan and on the analysis of the effectiveness of the implementation of new laws aimed at protecting personal data. This will help identify additional aspects for improving data protection and strengthening regulation.

Acknowledgements

None.

Conflict of interest

None.

References

- [1] Act of Japan No. 57 "On the Protection of Personal Information". (2003). Retrieved from <https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.
- [2] Akhmetbek, Y., & Špaček, D. (2021). Opportunities and barriers of using blockchain in public administration: The case of real estate registration in Kazakhstan. *NISPAcee Journal of Public Administration and Policy*, 14(2), 41-64. doi: 10.2478/nispa-2021-0014.
- [3] Akhmetova, S. (2023). *Some aspects of the personal data protection law in Kazakhstan*. Retrieved from <https://www.mondaq.com/data-protection/1332632/some-aspects-of-the-personal-data-protection-law-in-kazakhstan>.
- [4] Amanzholova, S., Akhmetova, D., & Sagymbekova, A. (2021). Development of a web-resources testing system for compliance with GDPR regulation. In *ICEMIS'21: The 7th international conference on engineering & MIS 2021* (pp. 1-6). Almaty: ACM Press. doi: 10.1145/3492547.3492661.
- [5] Bak, M., Madai, V.I., Fritzsche, M.C., Mayrhofer, M.T., & McLennan, S. (2022). You can't have AI both ways: Balancing health data privacy and access fairly. *Frontiers in Genetics*, 13, article number 929453. doi: 10.3389/fgene.2022.929453.
- [6] Brazilian General Data Protection Law. (2018, August). Retrieved from <https://surl.li/mybgqw>.

- [7] Chan, K., Chen, E., Heneghan, M., Soffer, D., & Wachirapornpruet, P. (2022). *Against the grain: The data regulatory regimes of Kazakhstan and Uzbekistan vis-à-vis Russia, China, and Big Tech*. London: Lse Ideas.
- [8] Code of Ethics and Business Conduct of Kaspi Bank JSC. (2025). Retrieved from https://cdn-kaspi.kz/kkz/rese/files/terms/code_of_ethics_and_business_conduct_of_kaspi_bank_jsc.pdf.
- [9] Directive of the European Parliament and of the Council No. 2002/58/EC “Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector” (Directive on Privacy and Electronic Communications). (2002, July). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058>.
- [10] E-commerce and online banking platform Kaspi. (2024). Retrieved from <https://www.Kaspi.kz>.
- [11] EU’s top court rules against targeted advertising on Facebook. (2023). Retrieved from <https://dig.watch/updates/eus-top-court-rules-against-targeted-advertising-on-facebook>.
- [12] Gal, M.S., & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, 16(3), 349-391. doi: 10.1093/joclec/nhaa012.
- [13] General Data Protection Regulation (GDPR). (2016, May). Retrieved from <https://gdpr-info.eu/>.
- [14] Gentile, G., & Lynskey, O. (2022). Deficient by design? The transnational enforcement of the GDPR. *International & Comparative Law Quarterly*, 71(4), 799-830. doi: 10.1017/S0020589322000355.
- [15] Gulyamov, S., & Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy*, 1(7), 1-32. doi: 10.59022/ijlp.119.
- [16] Iskakova, Zh.T., & Kadyrzhanova, T.S. (2022). *Analysis of problems and challenges in the legislation of the Republic of Kazakhstan on personal data protection and international legal regulation*. *Bulletin of L.N Gumilyov Eurasian National University, Law Series*, 141(4), 48-60.
- [17] Jones, M.L., & Kaminski, M.E. (2020). *An American’s guide to the GDPR*. *Denver Law Review*, 98(1), 93-128.
- [18] Kajcsa, A., & Dogaru, L. (2022). The challenges brought by GDPR to the use of intelligent systems. In L. Moldovan & A. Gligor (Eds.), *15th International conference interdisciplinarity in engineering: Conference proceedings* (pp. 298-306). Cham: Springer. doi: 10.1007/978-3-030-93817-8_29.
- [19] Kazakhstan strengthens personal data protection by gradually moving toward GDPR standards. (2021). Retrieved from <https://www.dentons.com/en/insights/alerts/2021/january/28/kazakhstan-strengthens-personal-data-protection-by-gradually-moving-toward-gdpr-standards>.
- [20] Khamidullina, Y. (2019). *Kazakhstan – the impact of the GDPR outside the EU*. Retrieved from <https://iuslaboris.com/insights/kazakhstan-the-impact-of-the-gdpr-outside-the-eu/>.
- [21] Kive, M., & Grasis, J. (2020). *Problems of application of the right to data portability*. *Acta Prosperitatis*, 11, 116-127.
- [22] Kocharyan, H., Vardanyan, L., Hamulák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, 21(2), 96-115. doi: 10.2478/iclr-2021-0015.
- [23] Kretschmer, M., Pennekamp, J., & Wehrle, K. (2021). Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)*, 15(4). doi: 10.1145/3466722.
- [24] Law of the Republic of Kazakhstan No. 18-8 “On Online Platforms and Online Advertising”. (2023, July). Retrieved from <https://adilet.zan.kz/eng/docs/Z2300000018>.
- [25] Law of the Republic of Kazakhstan No. 347-6 ZRC “On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan Regarding Regulation of Digital Technologies”. (2020, June). Retrieved from <https://adilet.zan.kz/rus/docs/Z2000000347>.
- [26] Law of the Republic of Kazakhstan No. 399-4 “On Introducing Amendments and Additions to Some Legislative Acts of the Republic of Kazakhstan on the Issues of Restoration of Economic Growth”. (2021, January). Retrieved from <https://adilet.zan.kz/rus/docs/Z2100000399>.
- [27] Law of the Republic of Kazakhstan No. 44-VIII “On Amending Certain Legislative Acts of the Republic of Kazakhstan on Information Security, Informatisation and Digital Assets”. (2023, December). Retrieved from <https://adilet.zan.kz/rus/docs/Z2300000044>.
- [28] Law of the Republic of Kazakhstan No. 508-2 “On Advertising”. (2003, December). Retrieved from https://adilet.zan.kz/eng/archive/docs/Z030000508_09.09.2024.
- [29] Law of the Republic of Kazakhstan No. 94-5 “On Personal Data and their Protection”. (2013, May). Retrieved from <https://adilet.zan.kz/eng/docs/Z1300000094>.
- [30] Lawson-Hetchely, C. (2022). *The potential impact of the future AI Act on the GDPR*. Oslo: University of Oslo.
- [31] Luisi, M. (2022). *GDPR as a global standards? Brussels’ instrument of policy diffusion*. Retrieved from <https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/>.
- [32] Lukings, M., & Lashkari, A.H. (2022). Comparative legal strategies. In *Understanding cybersecurity law in data sovereignty and digital governance: An overview from a legal perspective* (pp. 181-204). Cham: Springer. doi: 10.1007/978-3-031-14264-2_5.
- [33] Luxembourg DPA fines Amazon EUR 746 million for GDPR violations. (2021). Retrieved from <https://www.huntonak.com/privacy-and-information-security-law/luxembourg-dpa-fines-amazon-756-million-euros-for-gdpr-violations>.
- [34] Maulenov, K., Kudubayeva, S., Kaziyeva, N., Zharlykassov, B., & Turebayeva, R. (2024). Biometric access system with automatic registration and loyalty check in the system of recognition and database entry. *Information Security Journal*. doi: 10.1080/19393555.2024.2403458.
- [35] Mentukh, N., & Shevchuk, O. (2023). *Protection of information in electronic registers: Comparative and legal aspect*. *Law, Policy and Security*, 1(1), 4-17.
- [36] News Portal Tengrinews. (2024). <https://www.Tengrinews.kz>.

- [37] Nurbatyrova, R., Japarov, B., Apakhayev, N., Abdulaziz, B., & Khushkeldiyeva, S. (2024). Digital transformation of archives in the context of the introduction of an electronic document management system in Kazakhstan. *Preservation, Digital Technology and Culture*, 53(3), 147-155. doi: 10.1515/pdctc-2024-0017.
- [38] Open Dialog. (2021a). Retrieved from <https://dialog.egov.kz/blogs/all-questions/691916>.
- [39] Open Dialog. (2021b). Retrieved from <https://dialog.egov.kz/blogs/all-questions/715842>.
- [40] Open Dialog. (2022a). Retrieved from <https://dialog.egov.kz/blogs/all-questions/724888>.
- [41] Open Dialog. (2022b). Retrieved from <https://dialog.egov.kz/blogs/all-questions/727791>.
- [42] Penal Code of the Republic of Kazakhstan. (2014, July). Retrieved from <https://adilet.zan.kz/eng/docs/K1400000226>.
- [43] Platform for Selling and Buying Real Estate Krisha. (2024). <https://www.krisha.kz>.
- [44] Poelman, M., & Iqbal, S. (2021). Investigating the compliance of the GDPR: Processing personal data on a blockchain. In *2021 IEEE 5th International conference on cryptography, security and privacy (CSP)* (pp. 38-44). New York: Institute of Electrical and Electronics Engineers. doi: 10.1109/CSP51677.2021.9357590.
- [45] Porcelli, L., Mastroianni, M., Ficco, M., & Palmieri, F. (2024). A user-centered privacy policy management system for automatic consent on cookie banners. *Computers*, 13(2), article number 43. doi: 10.3390/computers13020043.
- [46] Prasad, A., & Perez, D.R. (2020). The effects of GDPR on the digital economy: Evidence from the literature. *Informatization Policy*, 27(3), 3-18. doi: 10.22693/NIAIP.2020.27.3.003
- [47] Presthus, W., & Sønslie, K.F. (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management*, 9(1), 38-53. doi: 10.12821/ijispm090102.
- [48] Prinsley, M.A., Yaros, O., Randall, R., & Hajda, O. (2020). *British Airways ultimately fined £20m for personal data breach by the UK ICO under the GDPR (reduced from £183.39m)*. Retrieved from <https://surl.li/aszrnc>.
- [49] Privacy Collective. (2020). *Oracle and salesforce taken to court in the Netherlands over GDPR infringement*. Retrieved from <https://edri.org/our-work/oracle-and-salesforce-taken-to-court-in-the-netherlands-over-gdpr-infringement/>.
- [50] Privacy Policy. (2025). Retrieved from <https://tengrinews.kz/page/confidential/>.
- [51] Prokk, B.C., & Schneider, I. (2021). *The geopolitical relevance of the GDPR*. Hamburg: University of Hamburg.
- [52] Regulation of the European Parliament and of the Council No. 2016/679 “On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive No. 95/46/EC (General Data Protection Regulation)”. (2016, April). Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [53] Regulation of the European Parliament and of the Council No. 2024/1689 “Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)” (2024, June). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>.
- [54] Santos, C., Rossi, A., Chamorro, L.S., & Bongard-Blanchy, K. (2021). Cookie banners, what's the purpose?: Analyzing cookie banner text through a legal lens. In *WPES'21: Proceedings of the 20th workshop on workshop on privacy in the electronic society* (pp. 187-194). New York: Association for Computing Machinery. doi: 10.1145/3463676.3485611.
- [55] Shtovba, O. (2024). Multi-armed bandit-based adaptive control of advertising in social networks. *Innovation and Sustainability*, 4(1), 83-92. doi: 10.31649/ins.2024.1.83.92.
- [56] The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR. (2022). Retrieved from <https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr>.
- [57] The CNIL's restricted committee imposes a financial penalty of EUR 50 million against GOOGLE LLC. (2019). Retrieved from <https://surl.li/yhwzav>.
- [58] Top Websites Ranking. (2024). Retrieved from <https://www.similarweb.com/top-websites/>.
- [59] Toqmadi, M., & Zakharchenko, N. (2021). I agree to terms and conditions: Negotiating privacy online in Central Asia. *JeDEM-EJournal of EDemocracy and Open Government*, 13(1), 71-100. doi: 10.29379/jedem.v13i1.633.
- [60] Veit, R.D. (2022). Safeguarding regional data protection rights on the global internet – the European approach under the GDPR. In M. Albers & I.W. Sarlet (Eds.), *Personality and data protection rights on the Internet: Brazilian and German approaches* (pp. 445-484). Cham: Springer. doi: 10.1007/978-3-030-90331-2_18.
- [61] Wiedemann, K. (2022). Profiling and (automated) decision-making under the GDPR: A two-step approach. *Computer Law & Security Review*, 45, article number 105662. doi: 10.1016/j.clsr.2022.105662.
- [62] Wodi, A. (2023). The EU General Data Protection Regulation (GDPR): Five years after and the future of data privacy protection in review. *SSRN*. doi: 10.2139/ssrn.4601142
- [63] Yakymenko, B. (2023). Formation of the institute of personal data protection and experience of its implementation in the countries of the EU. *Scientific Journal of the National Academy of Internal Affairs*, 28(4), 68-79. doi: 10.56215/naia-herald/4.2023.68.
- [64] Yerbolatov, Y.Y., Zhetpisov, S.K., Boretsky, A.V., Alibayeva, G.A., & Kolesnikov, Y.Y. (2022). Personal data protection in Kazakhstan and the EU: Comparative-legal analysis. *Journal of Sustainability Studies*, 12(1), 69-88. doi: 10.3280/RISS2022-001005.
- [65] Younas, A., Umarova, A., Hassan, A., & Usman, Z. (2020). *Overview of big data and cloud computing laws, regulations and policies in Central Asia*. Lahore: AI Mo Innovation Consultants Ltd. doi: 10.2139/ssrn.3672779.
- [66] Zaeem, R.N., & Barber, K.S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, 12(1). doi: 10.1145/3389685.
- [67] Zaki, H.O., Kamarulzaman, Y., & Mohtar, M. (2021). Cognition and emotion: Exploration on consumers response to advertisement and brand. *Jurnal Pengurusan*, 63, 1-14. doi: 10.17576/pengurusan-2021-63-05.

- [68] Zhetpissov, S., Mussabekova, N., Alibayeva, G., Dubovitskay, O., & Talipova, Zh. (2024). Vulnerability of personal data of Kazakhstani citizens and the need to implement the European experience. *Rivista di Studi sulla Sostenibilita*, 2, 305-323. doi: [10.3280/riss2024-002017](https://doi.org/10.3280/riss2024-002017).

Правове регулювання профілювання та таргетованої реклами в Казахстані крізь призму європейського досвіду

Сауле Ахметова

Кандидат юридичних наук

Казахський національний університет імені аль-Фарабі

050040, просп. Аль-Фарабі, 71, м. Алмати, Республіка Казахстан

<https://orcid.org/0009-0004-5393-4752>

Алуа Ібраєва

Доктор юридичних наук, професор

Казахський національний університет імені аль-Фарабі

050040, просп. Аль-Фарабі, 71, м. Алмати, Республіка Казахстан

<https://orcid.org/0000-0002-2946-6408>

Діна Баймаханова

Доктор юридичних наук, доцент

Казахський національний університет імені аль-Фарабі

050040, просп. Аль-Фарабі, 71, м. Алмати, Республіка Казахстан

<https://orcid.org/0000-0001-5903-9020>

Дінара Турсинкулова

Кандидат юридичних наук, доцент

Казахський національний університет імені аль-Фарабі

050040, просп. Аль-Фарабі, 71, м. Алмати, Республіка Казахстан

<https://orcid.org/0000-0003-4768-2048>

Томас Хоффманн

Доктор юридичних наук, доцент

Талліннський технічний університет

19086, дорога Ехітаджате, 5, м. Таллінн, Естонія

<https://orcid.org/0000-0003-4761-0722>

Анотація. Дослідження присвячене аналізу чинної нормативно-правової бази, що регулює профілювання і таргетовану рекламу в Казахстані, з урахуванням європейського досвіду. Дослідження включало огляд нормативно-правових актів Казахстану, що регулюють використання персональних даних, і порівняльний аналіз з положеннями Загального регламенту про захист даних. Аналіз продемонстрував, що хоча в Казахстані встановлені базові стандарти захисту персональних даних, рівень прозорості та контролю за процесом обробки даних залишається помітно нижчим порівняно з європейськими нормами. Основними проблемами є відсутність чіткої згоди користувачів на використання їхніх даних для таргетованої реклами, обмежені можливості для управління особистою інформацією, а також недостатні фінансові ресурси для застосування передових технологій і певні правові обмеження, спричинені жорсткою державною політикою. Аналіз казахстанських онлайн-платформ, зокрема таких, як Kaspi, Tengrinews і Krisha, показав, що процедури обробки даних на цих платформах не відповідають стандартам Загального регламенту про захист даних. Це створює юридичні ризики для бізнесу, особливо у зв'язку з потенційним виходом на європейський ринок. Результати дослідження підкреслили необхідність удосконалення національного законодавства у сфері захисту персональних даних. Рекомендується запровадити механізми, що забезпечують явну згоду користувача на обробку даних, підвищити прозорість політик конфіденційності, розширити права користувачів, зокрема можливість видаляти збережені дані та передавати їх. Приведення законодавства Казахстану у відповідність до європейських стандартів не тільки посилить захист прав громадян, а й підвищить конкурентоспроможність казахстанських компаній на міжнародній арені.

Ключові слова: обробка персональних даних; міжнародні стандарти; політика конфіденційності; цифровий ринок; захист прав користувачів