

8 Raghavan M., Barocas S., Kleinberg J., Levy K. *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices* // *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. – 2020. – P. 469–481. – doi: 10.1145/3351095.3372828.

9 Kellogg K.C., Valentine M.A., Christin A. *Algorithms at Work: The New Contested Terrain of Control* // *Academy of Management Annals*. – 2020. – Vol. 14, №1. – P. 366–410. – doi: 10.5465/annals.2018.0174.

10 Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L. *The Ethics of Algorithms: Mapping the Debate* // *Big Data & Society*. – 2016. – Vol. 3, № 2. – P. 1–21. – doi: 10.1177/2053951716679679.

11 Braidotti R. *The Posthuman*. – Cambridge: Polity Press, 2013. – 229 p.

12 Hayles N.K. *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. – Chicago: University of Chicago Press, 1999. – 366 p.

13 Floridi L. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. – Oxford: Oxford University Press, 2014. – 248 p.

14 Hui Y. *On the Existence of Digital Objects*. – Minneapolis: University of Minnesota Press, 2016. – 336 p.

15 Green A. *Artificial Intelligence and the Changing Demand for Skills in the Labour Market*. – OECD Artificial Intelligence Papers, № 14. – Paris: OECD Publishing, 2024. – doi: 10.1787/88684e36-en.

16 Brynjolfsson E., Chandar B., Chen R. *Canaries in the Coal Mine? Six Facts about the Recent Employment Effects of Artificial Intelligence*. – Stanford Digital Economy Lab Working Paper, 2025.

17 Felten E.W., Raj M., Seamans R. *Occupational, Industry, and Geographic Exposure to Artificial Intelligence: A Novel Dataset and Its Potential Uses* // *Strategic Management Journal*. – 2021. – Vol. 42, № 12. – P. 2195–2217. – doi: 10.1002/smj.3286.

18 Eloundou T., Manning S., Mishkin P., Rock D. *GPTs are GPTs: Labor Market Impact Potential of LLMs* // *Science*. – 2024. – Vol. 384, № 2. – P. 1306–1308. – doi: 10.1126/science.adj0998.

19 World Economic Forum. *The Future of Jobs Report 2025*. – Geneva: World Economic Forum, 2025.

IRSTI 04.51.54

DOI: <https://doi.org/10.51889/2959-6270.2026.94.2.008>

Zh. E. Zhapsarbayeva^{1*} , A.Sabitkyzy¹ 

¹ Abai Kazakh National Pedagogical University
Almaty, Kazakhstan

* e-mail: zhanna.zhapsarbayeva999@gmail.com

MEDIA EDUCATION AND DIGITAL MEDIA SECURITY OF KAZAKHSTANI YOUTH

Abstract

The article analyzes the sociological role of media education in strengthening digital media security among young people in Kazakhstan. The purpose of the study is to conceptualize media education not only as a set of technical skills or fact-checking procedures, but also as a social mechanism for developing informational resilience, responsible communication, and civic participation in a mediatized society. The article is based on a scientific-analytical design that combines conceptual analysis, problem-comparative interpretation, and theoretical model-building. The theoretical framework draws on media literacy studies, critical media education, mediatization theory, uses and gratifications research, communication power theory, and recent scholarship on misinformation and digital risks. Publicly available analytical data on Kazakhstan's digital

environment are used to situate the argument in the national context. The analysis shows that young people's digital media security should be understood as a three-level phenomenon: cognitive security, related to source evaluation and resistance to manipulation; institutional security, dependent on the coordination of education, family, media policy, and digital platforms; and ethical-communicative security, involving digital responsibility, personal data safety, and respectful online participation. The article argues that the rapid expansion of internet and social media use in Kazakhstan creates new educational and civic opportunities, while also increasing exposure to disinformation, emotional manipulation, algorithmic enclosure, and unsafe data practices. The scholarly contribution of the article lies in proposing a multi-level model of media education as a social infrastructure for youth media security.

Keywords: media education, media literacy, digital media security, youth, disinformation, digital environment, Kazakhstan.

Ж.Е. Жансарбаева^{1}, А.Сәбитқызы¹*

*¹ Абай атындағы Қазақ ұлттық педагогикалық университеті
Алматы, Қазақстан*

** e-mail: zhanna.zhapsarbayeva999@gmail.com*

ҚАЗАҚСТАН ЖАСТАРЫНЫҢ ЦИФРЛЫҚ МЕДИАҚАУІПСІЗДІГІ ЖӘНЕ ОНЫ ҚАЛЫПТАСТЫРУДАҒЫ МЕДИАБІЛІМНІҢ РӨЛІ

Аңдатпа

Мақалада Қазақстан жастарының цифрлық медиақауіпсіздігін қалыптастырудағы медиабілімнің социологиялық рөлі талданады. Зерттеудің мақсаты – медиабілімді тек техникалық дағды немесе ақпаратты тексеру тәсілі ретінде емес, медиатизацияланған қоғам жағдайындағы ақпараттық тұрақтылықты, жауапты коммуникацияны және азаматтық қатысуды қалыптастыратын әлеуметтік тетік ретінде негіздеу. Мақала ғылыми-аналитикалық зерттеу дизайнына сүйенеді; онда концептуалдық талдау, проблемалық-салыстырмалы түсіндіру және модельдеу тәсілдері біріктірілді. Теориялық негіз ретінде медиасауаттылық теориялары, сыни медиабілім тұжырымдамасы, медиатизация теориясы, аудиторияның медианы пайдалану уәждері туралы зерттеулер, коммуникациялық билік теориясы және жалған ақпарат мәселесіне арналған қазіргі ғылыми еңбектер пайдаланылды. Қазақстандағы цифрлық ортаға қатысты ашық аналитикалық деректер зерттеу контексін нақтылау үшін қолданылды. Талдау нәтижесінде жастардың цифрлық медиақауіпсіздігі үш деңгейлі құбылыс ретінде сипатталды: когнитивтік қауіпсіздік дереккөзді бағалау және манипуляцияға қарсы тұру қабілетімен; институционалдық қауіпсіздік білім беру, отбасы, медиасаясат және цифрлық платформалар арасындағы үйлесіммен; этикалық-коммуникативтік қауіпсіздік цифрлық жауапкершілік, дербес деректерді қорғау және онлайн қатысу мәдениетімен байланысты. Мақалада Қазақстанда интернет пен әлеуметтік желілердің кең таралуы жастарға білім алу, коммуникация және азаматтық қатысу мүмкіндіктерін кеңейткенімен, жалған ақпарат, эмоциялық манипуляция, алгоритмдік тұйықталу және деректер қауіпсіздігі тәуекелдерін күшейтетіні көрсетіледі. Мақаланың ғылыми үлесі – медиабілімді жастардың медиақауіпсіздігін қалыптастыратын көпдеңгейлі әлеуметтік инфрақұрылым ретінде ұсыну.

Түйін сөздер: медиабілім, медиасауаттылық, цифрлық медиақауіпсіздік, жастар, жалған ақпарат, цифрлық орта, Қазақстан.

Жапсарбаева Ж.Е.^{1*}, Сабитқызы А.¹.

¹ Казахский национальный педагогический университет имени Абая
Алматы, Казахстан

*e-mail : zhanna.zhapsarbayeva999@gmail.com

МЕДИАОБРАЗОВАНИЕ И ЦИФРОВАЯ МЕДИАБЕЗОПАСНОСТЬ КАЗАХСТАНСКОЙ МОЛОДЕЖИ

Аннотация

В статье рассматривается роль медиаобразования в формировании цифровой медиабезопасности молодежи Казахстана в условиях стремительного расширения цифровой коммуникации и возрастающей медиатизации общественной жизни. Актуальность исследования обусловлена двойственной природой цифровой среды: открывая перед молодежью новые образовательные, коммуникативные и гражданские возможности, она одновременно усиливает риски дезинформации, эмоциональной манипуляции, алгоритмической замкнутости и небезопасного обращения с персональными данными. Особая уязвимость молодого поколения связана с его интенсивной включенностью в цифровые практики и недостаточной сформированностью устойчивых навыков критического осмысления медиаконтента. В казахстанском контексте эти процессы приобретают особую значимость на фоне цифровизации образования и развития государственной молодежной политики, что усиливает потребность в системном формировании медиакомпетенций. Цель статьи заключается в теоретическом обосновании медиаобразования как социального механизма развития информационной устойчивости, критической рефлексии, ответственной коммуникации и гражданской субъектности молодежи. Исследование носит теоретико-концептуальный характер и основано на синтезе концепций медиаграмотности, критического медиаобразования, медиатизации, подхода «использования и удовлетворения», теории коммуникационной власти, а также современных исследований цифровых рисков и дезинформации. В результате предложена многоуровневая модель цифровой медиабезопасности молодежи, объединяющая когнитивный, институциональный и этико-коммуникативный уровни. Научная оригинальность статьи заключается в концептуализации медиаобразования как социальной инфраструктуры медиабезопасности молодежи в казахстанском обществе.

Ключевые слова: медиаобразование, медиаграмотность, медиабезопасность, молодежь, дезинформация, цифровая среда, Казахстан.

Introduction

Digital communication has changed the conditions under which people receive information, learn, express opinions, build identities, and participate in public life. Kazakhstan is deeply involved in this transformation. DataReportal's "Digital 2026: Kazakhstan" report states that there were 19.5 million internet users in Kazakhstan at the end of 2025, with internet penetration reaching 93.4 percent of the total population; the same report identifies 16.9 million social media user identities in October 2025 [1]. These figures should not be read as technical statistics alone. They indicate that digital communication has become an everyday social environment in which young people study, maintain relationships, consume news, respond to public events, and construct images of themselves and others.

The same process creates a new problem for sociology and education: media security can no longer be understood only as protection of networks, devices, and state information infrastructure. Technical cybersecurity remains necessary, yet it does not explain why young people trust misleading information, repost emotionally charged messages, reveal personal data, or remain within algorithmically narrowed information flows. Digital media security is therefore a question of social behavior, educational preparation, institutional coordination, and communicative ethics. A young person is not merely a recipient of messages produced by professional media. In the platform

environment, he or she is also a distributor, commentator, content producer, and visible participant in public communication.

UNESCO defines media and information literacy as a complex set of competencies that enables citizens to access, evaluate, use, create, and communicate information critically and ethically [2, p.112]. This definition is important because it moves media education beyond a narrow pedagogical interpretation and links it with democratic participation, social responsibility, and resilience to manipulation. Kazakhstan's cybersecurity agenda also emphasizes the importance of awareness, human capital, and the formation of information security culture [3]. However, a secure digital society cannot be built through infrastructure and regulation alone. It requires citizens who are able to assess sources, understand media formats, recognize manipulation, protect their personal data, and communicate responsibly.

The broader digital transformation of Kazakhstan strengthens the urgency of this issue. International assessments point to rapid development of online services, public-sector platforms, business digitalization, and connectivity in the country [4, p.13]. At the same time, the Bureau of National Statistics regularly publishes indicators on internet use, ICT purposes, and the digital literacy of the population, which confirms that digitalization is not only an economic or technological process but also a social one [5]. The sociological significance of this transformation lies in the fact that access to the internet does not automatically produce critical autonomy. A digitally connected young person may still remain vulnerable to misinformation, manipulative design, peer pressure, aggressive communication, or data extraction.

One of the most serious risks in this environment is the increasing complexity of disinformation. Wardle and Derakhshan describe information disorder as a broad phenomenon that includes misinformation, disinformation, and malinformation; each of these forms may damage public trust and distort collective understanding [6, p.57]. For young audiences, misleading content often arrives not through traditional news media, but through short videos, influencers, memes, messenger channels, comment threads, or algorithmically selected recommendations. This means that media education must go beyond the traditional task of teaching students to "read media texts". It should also help them understand platforms, visual persuasion, emotional framing, the interests of content producers, and the social mechanisms by which information circulates.

Scientific literature offers several approaches to this problem. Livingstone connects media literacy with access, analysis, evaluation, and content creation in the context of new communication technologies [7, p.9]. Buckingham argues that media education should not isolate young people from media culture, but should help them understand and critically engage with it [8, p.117]. Hobbs links digital and media literacy with classroom practice, civic participation, and cultural understanding [9, p.123]. Critical media literacy emphasizes that media texts are not neutral containers of information; they are constructed through social interests, power relations, commercial logic, and cultural codes [10, p. 61]. Together, these approaches make it possible to understand media education as a sociological mechanism that connects individual competence with institutional responsibility.

The purpose of this article is to analyze the role of media education in shaping digital media security among Kazakhstani youth. The article addresses the following research question: how can media education function as a social infrastructure that reduces digital risks and strengthens responsible media participation among young people in Kazakhstan? The analytical proposition is that media education contributes to media security only when it simultaneously develops cognitive skills, institutional support, and ethical-communicative responsibility. To develop this proposition, the article pursues three tasks: first, to clarify the conceptual relationship between media education and media security; second, to identify key digital risks affecting young people; and third, to propose a multi-level model of media education suitable for the Kazakhstani context.

Research methodology

This article is designed as a scientific-analytical study. It does not present the results of a new survey or interview project. Instead, it develops a conceptual and sociological interpretation based on

academic literature, international recommendations, official and open analytical data, and contemporary studies of misinformation. This design was chosen deliberately because digital media security is not a single measurable variable. It emerges at the intersection of technological infrastructure, media policy, education, platform architecture, family practices, civic culture, and everyday user behavior. Before conducting a narrower empirical measurement, it is necessary to clarify the structure of the problem, the categories used to describe it, and the mechanisms through which media education may influence youth media practices.

The empirical background of the article is limited to publicly available contextual data. The first contextual source is DataReportal's 2026 country report on Kazakhstan, which provides current indicators of internet penetration and social media use. The second contextual source is Kazakhstan's cybersecurity policy framework, which places human awareness and information security culture among the elements of national digital security. The third contextual source is the OECD analysis of Kazakhstan's digital transformation, which situates the country's digital development within broader institutional and economic reforms. The fourth contextual source is the Bureau of National Statistics, whose ICT tables include indicators such as the share of internet users, the purposes of internet use, and the level of digital literacy of the population. These sources do not replace field research, but they help explain why youth media security has become a sociologically relevant issue in Kazakhstan.

The academic source base was selected according to three criteria. The first criterion was theoretical significance. This group included works on media literacy, critical media education, participatory culture, mediatization, audience motivation, and communication power. These sources provide the conceptual framework for understanding young people not as passive recipients of media influence, but as active subjects who interpret, produce, and redistribute media content. The second criterion was explanatory relevance to contemporary informational risks. This group included studies of misinformation, fake news, psychological susceptibility to false information, correction effects, and media literacy interventions. The third criterion was applicability to educational and policy discussion. This group included international recommendations and studies that can inform curriculum design, media pedagogy, and civic education.

Three analytical procedures were used. First, conceptual analysis was applied to define the relationship between media education, media literacy, media security, disinformation, digital responsibility, and informational resilience. In this article, media education is understood as the organized process of developing knowledge, skills, values, and habits necessary for critical and responsible participation in media environments. Media literacy refers to the practical competencies that allow individuals to access, analyze, evaluate, create, and share information. Media security is understood as the condition in which individuals and institutions can participate in media communication without being systematically exposed to manipulation, harmful content circulation, unsafe data practices, or communicative aggression. Informational resilience refers to the capacity of individuals and groups to resist, correct, and recover from misleading or manipulative information.

Second, problem-comparative analysis was used to classify youth digital risks into cognitive, institutional, social, and ethical dimensions. Cognitive risks include false information, distorted context, weak source evaluation, and emotional persuasion. Institutional risks arise when schools, universities, families, media organizations, and public policy operate separately and fail to produce a coherent culture of media responsibility. Social risks include polarization, group pressure, online hostility, and the reduction of public discussion to emotional reactions. Ethical risks concern personal data, digital footprints, online reputation, and responsibility for shared content.

Third, model-building was used to formulate a three-level model of media education as a condition of digital media security. The model is not presented as a statistical typology. It is an analytical framework that can guide future empirical research, curriculum design, and policy discussion. It contains three interconnected levels: cognitive security, institutional security, and ethical-communicative security. Each level has its own educational mechanisms and expected social outcomes. This model is especially relevant for Kazakhstan because youth media practices are shaped by high digital connectivity, multilingual information flows, and strong platform-based communication.

The theoretical framework combines three lines of research. The first is media literacy theory, which focuses on competencies needed to access, evaluate, interpret, create, and share media content responsibly [11, p. 96]. The second is mediatization theory, which explains how media become embedded in social institutions and everyday life. Couldry and Hepp argue that social reality is increasingly constructed through mediated practices [12, p.110], while Hjarvard describes the media as agents of social and cultural change [13, p.128]. The third line is uses and gratifications research, which studies why audiences choose particular media and what needs these media fulfill [14, p.519]. This combination makes it possible to connect media security with youth motivation, institutional structures, and the cultural logic of platforms.

The limitation of the study should be clearly stated. Since the article does not include original respondent data, its conclusions should not be interpreted as statistical generalizations about all Kazakhstani youth. They are conceptual and analytical propositions grounded in existing literature and open contextual data. This limitation also defines the ethical status of the research: no personal data were collected, no minors or students were surveyed, and no confidential information was processed. The value of the article lies in clarifying the sociological logic of media education as a security resource and in proposing a framework that can be tested and developed in future empirical research.

Results

The analysis identifies digital media security of youth as a three-level phenomenon. The first level is cognitive security. It refers to the ability of young people to recognize the structure of a media text, evaluate the credibility of a source, compare evidence, identify emotional framing, and distinguish between argument, opinion, advertising, satire, manipulation, and deliberate fabrication. Tandoc, Lim, and Ling show that "fake news" is not a single genre but a broad label that covers several forms of problematic information, from satire and parody to fabricated content and manipulated context [15, p. 149]. This means that media education cannot teach young people to divide all information mechanically into "true" and "false". It must teach them to ask where a message comes from, who benefits from it, what evidence it uses, which emotions it activates, and how it circulates.

Cognitive security is especially important because false information often spreads through ordinary social mechanisms. The study by Vosoughi, Roy, and Aral demonstrated that false news can spread online more rapidly and widely than true news, partly because it is often more novel and emotionally engaging [16, p. 1148]. This finding is crucial for youth media education. Young users may share content not because they intend to mislead others, but because the content is surprising, humorous, morally charged, or consistent with the expectations of their peer group. Media education should therefore include exercises that help students pause before reposting, analyze the emotional architecture of a message, and recognize the difference between social excitement and evidential reliability.

The second level is institutional security. Young people's media behavior is not formed by individual choice alone. It is shaped by schools, universities, families, media organizations, state policy, platform algorithms, and the broader culture of public communication. In Kazakhstan, where digital participation is expanding and media consumption is multilingual, the coordination of these institutions becomes particularly important. If universities teach academic integrity but ignore social media literacy, if families warn children about online risks but lack practical knowledge of platform settings, or if public communication uses emotionally polarizing language, media education remains fragmented. Institutional security means that media education must become an integrated social practice rather than an occasional lecture or campaign.

The third level is ethical-communicative security. A young person in a digital environment does not merely receive information; he or she comments, shares, reacts, uploads, edits, and participates in discussions. Every action may influence other users, leave a digital trace, or contribute to the spread of harmful content. Therefore, media education should include digital etiquette, privacy awareness, data protection, online reputation, cyberbullying prevention, and responsible disagreement. Guess and colleagues show that even relatively brief digital media literacy interventions can improve people's ability to distinguish mainstream news from false news [17, p.15540]. Yet sustainable effects require

more than short interventions; they require a stable educational culture in which critical evaluation and responsible communication become routine practices.

A major result of the analysis is that youth vulnerability to misinformation should not be explained only by a lack of knowledge. Psychological research demonstrates that false beliefs are shaped by familiarity, emotional resonance, identity-protective reasoning, cognitive shortcuts, and insufficient analytical reflection [18, p.390]. Once a false belief is formed, it may resist later correction because people often retain the original mental model even after receiving a correction [19, p.17]. For this reason, media education should be preventive rather than merely reactive. Students should be introduced in advance to common manipulation techniques, such as false authority, misleading headlines, decontextualized statistics, emotional fear appeals, fabricated cause-and-effect relations, and artificial amplification through coordinated sharing.

The second result concerns the practical translation of media literacy into habits. Kozyreva and colleagues describe a toolbox of individual-level interventions against online misinformation, including accuracy prompts, prebunking, inoculation, source evaluation, and friction mechanisms that slow down impulsive sharing [20, p. 1048]. These tools are useful for media education in Kazakhstan because they transform abstract critical thinking into repeated practices. A student should be able to ask: Is the source identifiable? Is the claim supported by evidence? Is the image used in its original context? Does the headline correspond to the text? Am I sharing this because it is reliable, or because it confirms what I already believe? Such questions help media education become a daily habit rather than a formal topic.

The Kazakhstani context adds several specific features to this model. First, young people operate in a multilingual media environment where Kazakh, Russian, English, and other-language content coexist. A single event may be framed differently across linguistic spaces, and these differences may influence trust, identity, and political perception. Second, youth media consumption is strongly platform-based. Short videos, messenger channels, influencers, and recommendation systems often shape attention more directly than traditional editorial media. Third, digital participation is tied to social visibility: students use platforms not only to learn or receive news, but also to present themselves, maintain friendships, and belong to communities. These features make media security a social and cultural issue, not only a technological one.

The third result is that media education must be linked with social inequality. High internet penetration does not automatically mean equal digital competence. The presence of national statistical indicators on internet use and digital literacy suggests that digital participation can be measured and compared, but it also reminds researchers that differences by region, age, language, education, and social environment may matter. A student in a large city may have stable access to diverse information sources and educational support, while another student may rely mainly on a limited set of social platforms or messenger groups. Media education should therefore be sensitive not only to general youth culture, but also to unequal conditions of access, interpretation, and support.

The fourth result concerns the relationship between media education and trust. Digital media security is not achieved by teaching young people to distrust everything. Total suspicion can be as harmful as naive trust because it may produce cynicism, withdrawal from public discussion, or attraction to conspiracy thinking. The educational aim should be calibrated trust: the ability to distinguish between reliable and unreliable sources, between institutional information and manipulative imitation, between evidence-based criticism and emotionally attractive misinformation. This is why media education should combine critical analysis with civic responsibility. It should not only identify risks, but also strengthen the capacity to participate constructively in public communication.

The results can be summarized in the following model. Media education contributes to digital media security when it simultaneously develops cognitive skills, institutional support, and ethical-communicative responsibility. If one of these dimensions is missing, the model becomes incomplete. Cognitive skills without institutional support remain individual and unstable. Institutional programs without ethical reflection become formal and bureaucratic. Ethical appeals without analytical tools

turn into general moral instruction. The strength of media education lies in combining these dimensions into a coherent infrastructure for responsible digital participation.

1-Table. Media education mechanisms for strengthening youth digital media security

Digital risk	Media education response	Expected social outcome
False or decontextualized information	Comparison of sources, identification of authorial interest, fact-checking routines, and evidence evaluation.	Critical assessment of information and reduced circulation of unreliable content.
Algorithmic enclosure and one-sided information flows	Explanation of platform logic, recommendation systems, and the need to use diverse sources.	Greater acceptance of informational plurality and lower dependence on narrow feeds.
Emotional manipulation and viral content	Analysis of headlines, visuals, emotional language, fear appeals, and moral outrage techniques.	Less impulsive sharing and more reflective media consumption.
Unsafe personal data practices and digital footprints	Training on privacy settings, online reputation, data protection, consent, and platform responsibility.	Safer digital behavior and stronger personal responsibility.
Online aggression and weak discussion culture	Education in digital ethics, respectful disagreement, cyberbullying prevention, and civic dialogue.	More responsible online participation and stronger civic media culture.
Fragmented institutional responsibility	Coordination of school, university, family, media organizations, and public policy.	Stable media education infrastructure rather than isolated campaigns.

Note - Compiled by the author on the basis of theoretical and analytical systematization.

The table demonstrates that media education should be treated as a social infrastructure rather than a narrow set of technical skills. Infrastructure here does not refer only to devices, networks, or digital platforms. It includes curricula, teacher competence, university policies, family communication practices, public information standards, platform transparency, and civic habits. In this sense, media education is a soft but long-term security mechanism. It does not aim to isolate young people from the media environment; it aims to make them capable of acting within it consciously, critically, and responsibly.

Now let's give some recommendations for research. First, media education should be introduced not only as a separate discipline but also as an interdisciplinary module. In sociology, students can study digital communities, online inequality, and public opinion on social platforms. In political science, they can analyze propaganda, information manipulation, political communication, and public trust. In law-related courses, attention can be given to personal data, copyright, and digital rights. In psychology, students can examine emotional persuasion, cognitive biases, and group influence. This approach prevents media education from becoming a narrow technical topic and turns it into a broad academic practice.

Second, universities should create practical media environments for students. Fact-checking clubs, student media laboratories, podcast and video studios, public communication workshops, and seminars on visual manipulation would allow students to develop media literacy through action. Small tasks may be especially effective: checking the origin of an image, comparing a headline with the full

text, identifying false statistics, analyzing the emotional tone of a short video, or tracing how a claim travels across platforms. These exercises connect theory with students' everyday media experience.

Third, media education should be linked with family and civic media culture. Young people's digital behavior is shaped not only in the classroom, but also in family conversations, messenger groups, peer networks, and responses to public events. Open lectures, brief guides for parents, school-university projects, and local information safety weeks can expand the social effect of media education. The aim is not surveillance of young people, but the formation of a shared culture of responsible digital communication.

Fourth, the effectiveness of media education should be assessed through practical indicators. It is not enough to test whether a student knows a theoretical definition. Assessment should include the ability to compare sources, detect questionable claims, explain emotional manipulation, protect personal data, cite properly, and participate ethically in digital discussion. If such indicators are adopted, media education can become a measurable and improvable element of Kazakhstan's media security policy.

For practical implementation, the proposed approach can be organized as a sequence of three educational stages. The first stage is diagnostic. Universities may assess students' initial media practices through anonymous classroom tasks: comparison of two news items, identification of the source of an image, recognition of manipulative headlines, or explanation of why a particular post seems persuasive. This does not require collecting sensitive personal data; it is enough to observe typical difficulties in source evaluation and argument analysis.

The second stage is formative. Students should work with real but ethically selected media examples: public news, open social media posts, screenshots with personal information removed, educational videos, and official data visualizations. The purpose is not to accuse young people of being vulnerable, but to show how ordinary media formats can guide attention and emotions. At this stage, the teacher's role is to move students from immediate reaction to reflective interpretation.

The third stage is evaluative. Media education should be assessed through applied outcomes rather than through memorization of definitions. A student can be considered media-literate when he or she can explain why a source is trustworthy or doubtful, compare several frames of the same event, identify missing context, avoid spreading unverified information, protect personal data, and conduct disagreement without verbal aggression. These indicators may be included in university quality assurance systems, student project assessment, and civic education programs.

Such an implementation pathway makes media education suitable for the Kazakhstani higher education context. It does not require the creation of an entirely new institutional system; rather, it strengthens existing courses, student activities, and public communication practices. The key condition is continuity: one lecture on fake news is not enough, while repeated analytical exercises across different disciplines can gradually form stable media habits.

A further step is to connect media education with student research activity. Students may prepare small analytical portfolios in which they compare media coverage of one social issue across several platforms, languages, and genres. Such portfolios can include a short description of the source, the type of evidence used, the emotional tone of the message, the possible audience, and the ethical risks of reposting. This format is useful because it does not require complex laboratory equipment, but it develops the central abilities required for media security: comparison, interpretation, verification, and responsible judgment.

The proposed recommendations also require teacher training. If teachers themselves are not confident in working with platform algorithms, visual content, AI-generated texts, and misinformation techniques, media education may remain formal. Therefore, professional development programs for university teachers should include practical modules on digital source verification, data ethics, visual literacy, and responsible use of artificial intelligence in education. This would connect media security with the modernization of higher education rather than treating it as a separate disciplinary topic.

Finally, institutional monitoring should be qualitative as well as quantitative. Universities may track not only the number of media literacy events, but also the quality of student projects, the

diversity of sources used in academic work, the ability to justify information choices, and the ethical tone of online discussions. These indicators make media education visible as a real component of educational quality.

Discussion

The findings support the view that media education should be treated as a core condition of digital media security rather than as an optional educational addition. Traditional security thinking often begins with the identification of external threats and the search for instruments of restriction, control, or defense. In the digital media environment, however, risks do not always come from an external adversary. They may also arise from routine user practices: rapid reposting, emotional reaction, uncritical trust in familiar sources, weak privacy habits, and participation in aggressive online communication. For this reason, media security policy should not be based only on distrust of youth behavior; it should strengthen the autonomy, judgment, and responsibility of young users.

This argument challenges the outdated model of the audience as a passive object of media influence. Young people use media for different purposes: to obtain information, relax, communicate, construct identity, gain recognition, join communities, and express civic positions. Uses and gratifications theory helps explain why a single platform can serve several social functions at once. A student may open the same application for entertainment, news, academic communication, and emotional support. If media education ignores these motives, it becomes abstract and moralizing. If it starts from the actual media life of students, it becomes socially meaningful and pedagogically effective.

The mediatization perspective further clarifies why media education cannot remain limited to journalism or computer science courses. Media logic increasingly influences politics, education, family communication, cultural identity, and public trust. In a mediatized society, citizens encounter reality through screens, feeds, platforms, search engines, and recommender systems. Therefore, media literacy is not only the skill of analyzing a media text. It is the ability to understand how social reality is selected, framed, circulated, and emotionally intensified through media technologies. For young people, this ability becomes part of broader socialization.

The works of Castells and Luhmann strengthen this interpretation. Castells argues that communication power in the network society is exercised through the programming of networks, control over attention, and the framing of meaning [22, p.571]. Luhmann shows that mass media participate in the social construction of reality by selecting what becomes visible and communicable [23, p.154]. Applied to youth media security, these ideas suggest that the most important question is not only whether a young person can identify one false message. The broader question is whether he or she understands how visibility, attention, credibility, and emotional resonance are produced in digital communication.

For Kazakhstan, this question has practical urgency. The country has a high level of digital connectivity, and young people are actively included in platform-based communication. At the same time, the national digital context cannot be reduced to a single homogeneous audience. Linguistic diversity, regional differences, variations in educational resources, and unequal family media practices may shape how young people understand and evaluate information. The Bureau of National Statistics' ICT indicators provide an important basis for future empirical analysis because they allow researchers to connect digital literacy and internet use with broader social conditions. This article therefore proposes not to speak about "Kazakhstani youth" as a completely uniform group, but to analyze youth media security through differentiated social contexts.

The multilingual character of Kazakhstan's media environment deserves special attention. Young people may consume Kazakh-language, Russian-language, English-language, and global platform content within the same day. Each linguistic space may contain its own trusted voices, emotional frames, political vocabulary, and cultural references. A news item, public scandal, or social conflict can be interpreted differently depending on language, platform, and audience. Media education should help students compare these frames without turning linguistic diversity into suspicion or conflict. For

example, classroom tasks may ask students to analyze how the same issue is presented in different language environments, what is emphasized or omitted, and which emotional strategies are used.

The educational system has a central role in this process. Yet it would be insufficient to assign media education only to informatics, journalism, or pedagogy courses. Digital media literacy should be integrated across sociology, political science, law, psychology, language education, cultural studies, and civic education. Sociology can help students analyze online communities and digital inequality; political science can examine propaganda, agenda-setting, and public trust; law can address data protection and copyright; psychology can explain cognitive biases and emotional manipulation; cultural studies can interpret symbols, identities, and representations. Such interdisciplinarity corresponds more closely to the complexity of digital media risks.

International educational research confirms the importance of digital reading, source comparison, and online information evaluation. OECD's work on 21st-century readers emphasizes that literacy in a digital world includes the ability to navigate multiple texts, assess credibility, and deal with conflicting information [21, p.216]. This is relevant for Kazakhstan because digital literacy is no longer separate from academic literacy. Students increasingly work with academic texts, news materials, social media posts, visual content, and generative artificial intelligence outputs. They must learn to cite correctly, verify sources, identify fabricated references, evaluate data visualizations, and use digital tools ethically. In this sense, media education becomes part of the broader culture of responsible knowledge production.

At the same time, media education should not become a prohibitive or punitive practice. Messages such as "do not trust", "do not watch", or "do not share" may create fear but do not develop stable judgment. More effective media education teaches students to ask questions: Who produced this message? What evidence does it contain? Why does it make me angry or afraid? What is missing from this frame? What may happen if I share it? Who may be harmed? Such questions transform media education from a set of prohibitions into a practice of reflective citizenship.

The family and platform dimensions should not be ignored. Many media habits are formed outside formal education: in family chats, peer groups, entertainment platforms, and influencer communities. Universities can strengthen media security only if their efforts are supported by wider civic media culture. Public lectures, parent-oriented guides, student media laboratories, fact-checking clubs, and partnerships with media organizations can extend media education beyond the classroom. Platform accountability is also important: privacy settings, transparent recommendation logic, reporting mechanisms, and age-appropriate safety tools influence how young people experience digital space. Media education is therefore most effective when it becomes a shared responsibility rather than an individual burden placed only on students.

The proposed model has a policy implication. If media education is treated as a single course, its effect will remain limited. If it is treated as a cross-institutional infrastructure, it can connect curriculum development, teacher training, youth policy, public communication, and digital platform regulation. This does not mean replacing free communication with excessive control. Rather, it means creating conditions in which young people are able to participate in digital life without becoming easy targets of manipulation, hostility, or unsafe data practices. In this sense, media education supports both security and freedom: it reduces vulnerability while preserving agency.

Conclusion

This article analyzed the role of media education in shaping digital media security among Kazakhstani youth. The main conclusion is that media security should not be understood only as a technical or administrative issue. It is directly connected with the ability of young people to understand information, evaluate evidence, communicate responsibly, protect personal data, and act consciously in digital environments. Media education is therefore not an auxiliary instrument of security; it is one of its social foundations.

The analysis identified three key functions of media education. The first is cognitive: source evaluation, recognition of manipulation, and assessment of evidence. The second is institutional:

coordination between schools, universities, families, media organizations, platforms, and public policy. The third is ethical-communicative: online responsibility, discussion culture, digital footprint awareness, and safe data practices. In Kazakhstan, a model that combines these three dimensions can strengthen young people's informational resilience and contribute to the development of civic media culture.

The scientific contribution of the article is the proposed three-level model of media education as a social infrastructure of youth media security. The model connects individual competencies with institutional conditions and ethical norms of communication. Future research should move in two directions. The first is empirical study of youth media practices in Kazakhstan across regions, languages, educational levels, and social groups. The second is evaluation of existing media education programs in schools and universities. Such research would make it possible to measure the actual effectiveness of media education and to transform it into a stable component of national media security policy.

References:

- 1 Kemp S. *Digital 2026: Kazakhstan* [Electronic resource] - DataReportal, 2025. - URL: <https://datareportal.com/reports/digital-2026-kazakhstan> (accessed: 22.05.2026).
- 2 Grizzle A., Wilson C., Tuazon R., Cheung C. K., Lau J., Fischer R., Gordon D. *Media and information literate citizens: think critically, click wisely! Media and information literacy curriculum for educators and learners*. - Paris: UNESCO, 2021. - 403 p.
- 3 Government of the Republic of Kazakhstan. Resolution No. 407 of June 30, 2017 'On Approval of the Cybersecurity Concept ("Cyber Shield of Kazakhstan")' [Electronic resource]. - URL: <https://adilet.zan.kz/rus/docs/P1700000407> (accessed: 22.05.2026).
- 4 OECD. *Improving Framework Conditions for the Digital Transformation of Businesses in Kazakhstan*. - Paris: OECD Publishing, 2023. - 75 p. - DOI:10.1787/368d4d01-en.
- 5 Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan. *Information and communication technologies and communications: dynamic tables* [Electronic resource]. - 2026. - URL: <https://stat.gov.kz/en/industries/business-statistics/stat-it/dynamic-tables/> (accessed: 22.05.2026).
- 6 Wardle C., Derakhshan H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. - Strasbourg: Council of Europe, 2017. - 109 p.
- 7 Livingstone S. *Media literacy and the challenge of new information and communication technologies* // *The Communication Review*. - 2004. - Vol. 7, № 1. - P. 3-14. - DOI: 10.1080/10714420490280152.
- 8 Buckingham D. *Media Education: Literacy, Learning and Contemporary Culture*. - Cambridge: Polity Press, 2003. - 219 p.
- 9 Hobbs R. *Digital and Media Literacy: Connecting Culture and Classroom*. - Thousand Oaks: Corwin, 2011. - 232 p.
- 10 Kellner D., Share J. *Critical media literacy is not an option* // *Learning Inquiry*. - 2007. - Vol. 1, № 1. - P. 59-69. - DOI:10.1007/s11519-007-0004-2.
- 11 Jenkins H., Purushotma R., Weigel M., Clinton K., Robison A. J. *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century*. - Cambridge, MA: MIT Press, 2009. - 145 p.
- 12 Couldry N., Hepp A. *The Mediated Construction of Reality*. - Cambridge: Polity Press, 2017. - 256 p.
- 13 Hjarvard S. *The mediatization of society: A theory of the media as agents of social and cultural change* // *Nordicom Review*. - 2008. - Vol. 29, № 2. - P. 105-134. - DOI: 10.1515/nor-2017-0181.
- 14 Katz E., Blumler J. G., Gurevitch M. *Uses and gratifications research* // *Public Opinion Quarterly*. - 1973. - Vol. 37, № 4. - P. 509-523. - DOI: 10.1086/268109.

- 15 Tandoc E. C. Jr., Lim Z. W., Ling R. Defining 'fake news': A typology of scholarly definitions // *Digital Journalism*. - 2018. - Vol. 6, № 2. - P. 137-153. - DOI: 10.1080/21670811.2017.1360143.
- 16 Vosoughi S., Roy D., Aral S. The spread of true and false news online // *Science*. - 2018. - Vol. 359, No. 6380. - P. 1146-1151. - DOI: 10.1126/science.aap9559.
- 17 Guess A. M., Lerner M., Lyons B., Montgomery J. M., Nyhan B., Reifler J., Sircar N. A digital media literacy intervention increases discernment between mainstream and false news in the United States and India // *Proceedings of the National Academy of Sciences*. - 2020. - Vol. 117, № 27. - P. 15536-15545. - DOI: 10.1073/pnas.1920498117.
- 18 Pennycook G., Rand D. G. The psychology of fake news // *Trends in Cognitive Sciences*. - 2021. - Vol. 25, № 5. - P. 388-402. - DOI: 10.1016/j.tics.2021.02.007.
- 19 Ecker U. K. H., Lewandowsky S., Cook J., Schmid P., Fazio L. K., Brashier N., Kendeou P., Vraga E. K., Amazeen M. A. The psychological drivers of misinformation belief and its resistance to correction // *Nature Reviews Psychology*. - 2022. - Vol. 1. - P. 13-29. - DOI: 10.1038/s44159-021-00006-y.
- 20 Kozyreva A., Lorenz-Spreen P., Herzog S. M., Ecker U. K. H., Lewandowsky S., Hertwig R. et al. Toolbox of individual-level interventions against online misinformation // *Nature Human Behaviour*. - 2024. - Vol. 8, № 6. - P. 1044-1052. - DOI: 10.1038/s41562-024-01881-0.
- 21 OECD. *21st-Century Readers: Developing Literacy Skills in a Digital World*. - Paris: OECD Publishing, 2021. - 216 p. - DOI: 10.1787/a83d84cb-en.
- 22 Castells M. *Communication Power*. - Oxford: Oxford University Press, 2009. - 571 p.
- 23 Luhmann N. *The Reality of the Mass Media*. - Stanford: Stanford University Press, 2000. - 154 p.