



**ҚЫЛМЫСТЫҚ ҚҰҚЫҚ. ҚЫЛМЫСТЫҚ процесс / Criminal law.
Criminal procedure/ Уголовное право. Уголовный процесс**

Scientific article

<https://doi.org/10.32523/2616-6844-2026-156-3-201-219>

IRSTI 10.77.51

Criminal law measures against digital forms of violence: An analysis of the current legislation of the Republic of Kazakhstan and its compliance with the contemporary challenges of societal digitalization

A.Zh. Muratova¹, L. Lantero², N.M. Apsimet^{*3}

¹L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

²European Public Law Organisation, European Law and Governance School, Rome, Italy

³Al-Farabi Kazakh National University, Almaty, Kazakhstan

(e-mail: ¹muratova_azh@enu.kz, ²l.lantero@cimea.it, ³apsimet.nurdaulet@gmail.com)

Abstract. Rapid digitization of society has led to a significant shift of interpersonal aggression online, making countermeasures against digital violence a highly relevant task for Kazakhstan. This paper provides a legal, comparative, and statistical analysis of protective legislation, primarily Article 115-1 of the Penal Code (stalking) and Article 127-2 of the Code of Administrative Offences (bullying of minors). The aim of the study is to evaluate whether existing criminal and administrative measures meet contemporary challenges. Utilizing formal-legal, comparative, and systemic methods, the authors present an original age-neutral definition of digital violence and substantiate the fragmentary nature of the current protective framework. It establishes that the material construction of stalking requiring "substantial harm" blocks early intervention, while restricting cyberbullying provisions to minors leaves adults unprotected. Drawing on the experience of Germany, Italy, France, and the EU, the authors advance de lege ferenda proposals: reconstructing Article 115-1 as a formal offence, extending cyberbullying liability to adults, criminalizing cyberflashing under a consent model, and imposing a procedural duty on providers to preserve deleted digital evidence prior to its transfer to law enforcement. The conclusions are tested against official enforcement data for 2025–2026 and a case study of 2025 judgments on pursuit-type conduct.

Keywords: digital violence, cyberbullying, stalking, cyberstalking, criminal liability, psychological violence, de lege ferenda

А.Ж. Муратова¹, Л. Лантеро², Н.М. Апсимет^{*3}

¹Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

²Еуропалық қоғамдық құқық ұйымы, Еуропалық құқық және басқару мектебі,
Рим, Италия

³әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
(e-mail: ¹muratova_azh@enu.kz, ²l.lantero@cimea.it, ³apsimet.nurdaulet@gmail.com)

**Цифрлық зорлық-зомбылыққа қарсы қылмыстық-құқықтық шаралар:
Қазақстан Республикасының қолданыстағы заңнамасын талдау және оның
қоғамды цифрландыру жағдайындағы өзектілігі**

Аңдатпа. Қоғамның қарқынды цифрлануы тұлғааралық агрессияның едәуір бөлігінің онлайн-ортаға ауысуына әкеліп, цифрлық зорлық-зомбылыққа қарсы іс-қимыл мәселесін Қазақстан Республикасы үшін аса өзекті етті. Мақалада елдің қорғау заңнамасына, ең алдымен ҚР ҚК 115-1-бабына (сталкинг) және ҚР ӘҚБтК 127-2-бабына (кәмелетке толмағанды жәбірлеу) кешенді құқықтық, салыстырмалы және статистикалық талдау жүргізіледі. Зерттеудің мақсаты – қолданыстағы қылмыстық-құқықтық және әкімшілік-құқықтық шаралардың цифрлық дәуірдің заманауи сын-қатерлеріне сәйкестігін бағалау. Формальды-заңдық, салыстырмалы-құқықтық және жүйелік әдістер негізінде жұмыста алғаш рет жәбірленушінің жасымен шектелмейтін цифрлық зорлық-зомбылықтың авторлық анықтамасы ұсынылып, қолданыстағы қорғау механизмінің фрагменттік сипаты дәлелденді. Сталкингтің «елеулі зиянға» байланыстырылған материалдық құрамы ерте сатыда араласуды шектейтіні, ал кибербуллинг туралы норманың тек кәмелетке толмағандармен шектелуі ересектерді құқықтық қорғаусыз қалдыратыны анықталды. Германия, Италия, Франция және Еуропалық одақ тәжірибесіне сүйене отырып, *de lege ferenda* ұсыныстары тұжырымдалды: 115-1-бапты формальды құрам ретінде қайта құру, кибербуллинг үшін жауаптылықты ересектерге тарату, киберфлешинг үшін қылмыстық жауаптылық белгілеу, онлайн-платформаларды пайдалануды саралаушы белгі ретінде енгізу, сондай-ақ провайдерлердің жойылған цифрлық іздерді құзыретті органдарға бергенге дейін сақтау процестік міндетін бекіту. Тұжырымдар 2025-2026 жылдарғы ресми құқық қолдану деректерімен және қудалау сипатындағы әрекеттер бойынша 2025 жылғы сот үкімдерін талдау арқылы тексерілді.

Түйін сөздер: цифрлық зорлық-зомбылық, кибербуллинг, сталкинг, киберсталкинг, қылмыстық жауаптылық, психологиялық зорлық-зомбылық, *de lege ferenda*

А.Ж. Муратова¹, Л. Лантеро², Н.М. Апсимет^{*3}

¹Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан

²Организация европейского публичного права, Школа европейского права и управления, Рим, Италия

³Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
(e-mail: ¹muratova_azh@enu.kz, ²l.lantero@cimea.it, ³apsimet.nurdaulet@gmail.com)

Уголовно-правовые меры противодействия цифровым формам насилия: анализ действующего законодательства Республики Казахстан и его соответствие современным вызовам цифровизации общества

Аннотация. Стремительная цифровизация общества обусловила перенос значительной части межличностной агрессии в онлайн-среду, превратив противодействие цифровому насилию в актуальную задачу для Республики Казахстан. В статье проводится комплексный правовой, сравнительный и статистический анализ охранительного законодательства страны, прежде всего ст. 115-1 УК РК (сталкинг) и ст. 127-2 КоАП РК (травля несовершеннолетних). Цель исследования – оценить соответствие действующих уголовно-правовых и административно-правовых мер современным вызовам цифровой эпохи. На основе формально-юридического, сравнительно-правового и системного методов в работе впервые дано авторское определение цифрового насилия, не ограниченное возрастом потерпевшего, и доказан фрагментарный характер существующего механизма защиты. Установлено, что материальный состав сталкинга, требующий наступления «существенного вреда», блокирует превентивное вмешательство на ранних стадиях, а ограничение нормы о кибербуллинге несовершеннолетними оставляет совершеннолетних граждан без правовой защиты. С опорой на опыт Германии, Италии, Франции и Европейского союза сформулированы предложения *de lege ferenda*: реконструкция ст. 115-1 УК РК в формальный состав, распространение ответственности за кибербуллинг на взрослых, криминализация киберфлешинга на основе модели согласия, введение квалифицирующего признака совершения деяния через онлайн-платформы, а также закрепление процессуальной обязанности интернет-провайдеров по сохранению удаленных цифровых следов до их передачи правоохранительным органам. Выводы проверены на официальных правоприменительных данных за 2025-2026 гг. и материалах судебной практики 2025 г. по делам о преследовании.

Ключевые слова: цифровое насилие, кибербуллинг, сталкинг, киберсталкинг, уголовная ответственность, психологическое насилие, *de lege ferenda*

Introduction

Digital tools mediate much of social life, allowing interpersonal aggression to follow victims beyond physical spaces. Traditional criminal-law categories do not always capture this conduct or its psychological effects. International data show reported lifetime exposure to cyberbullying rising from 18% in 2007 to 36% in 2019 [1].

In Kazakhstan, scholarly literature reports 139 child suicides in 2025 and associates school bullying with nearly one-fifth of cases; the Children's Rights Ombudsman estimates its share

among contributing factors at 22% [2]. These figures underscore the need to examine the legal response to harassment, including online conduct.

Kazakhstan adopted two relevant reforms. Article 127-2 of the Code of Administrative Offences, introduced in 2024, addresses bullying and cyberbullying of minors and, in specified cases, the responsibility of guardians [3]. Article 115-1 of the Penal Code, introduced in 2025, criminalizes unlawful pursuit as a criminal misdemeanor without restricting the mode of pursuit [4].

Enforcement data record 121 offences connected with bullying of minors in January-October 2024 [5] and 248 registered stalking cases in the first five months of 2026 [13]. Such figures reflect reporting and enforcement practices, not the prevalence of digital violence.

The relationship between Articles 115-1 and 127-2, the limits of their protection and their suitability for digitally mediated aggression require systematic assessment. This study addresses those questions.

Research methods and materials

The legal materials comprise the Penal Code (Articles 3, 10, 15, 71, 98-3, 115, 115-1, 131 and 147) [4], the Code of Administrative Offences (Article 127-2) [3], the child-rights legislation [6], the amending laws introducing stalking and bullying provisions [7; 8], and laws on personal data and online platforms [33; 34]. Comparative sources are the criminal laws of Germany, Italy, France and England and Wales [10; 22; 23; 32], the EU Digital Services Act and e-Evidence Regulation [11; 12; 30], and the Budapest Convention [31]. The study also draws on Kazakhstani doctrine [9; 14–16] and international research on technology-facilitated abuse, online harm, cyberbullying and content detection [2; 12; 17–20].

The empirical material consists of official enforcement figures for Article 115-1 from its entry into force on 20 August 2025 to June 2026 [13; 24; 25], and data on Article 127-2 for January–October 2024 [5]. In September 2026, a search of the Supreme Court’s judicial-act database found no publicly available judgments under Article 115-1. The study therefore examines four first-instance judgments under Article 115 (threat) from 2025 [26–29]. They involve repeated digital contact or surveillance akin to pursuit and illustrate classification, proof, and sanctions; parties’ names are omitted.

Formal-legal analysis identifies the elements of the existing and proposed offences; comparative analysis tests the suitability of foreign models for Kazakhstan; descriptive statistics characterize registered cases; case studies examine judicial treatment of pursuit; and systemic analysis identifies overlaps and gaps. Registration figures reflect reporting and enforcement, are not separated by online and offline conduct, and do not identify the missing elements in terminated cases. They cannot establish actual prevalence or the cause of case termination.

Findings

1. Kazakhstani law has no unified category of digital violence. Article 127-2 addresses bullying of minors administratively, whereas Article 115-1 criminalizes stalking without an age restriction [3; 4]. Drawing on technology-facilitated abuse research [17], this study defines digital violence as deliberate use of information and communication technologies against a person’s will to violate psychological integrity, restrict freedoms or degrade honour and dignity.

2. Article 115-1 fills a gap concerning unlawful pursuit, but its requirement of «substantial harm» may impede early intervention [4; 9]. In the first five months of 2026, 101 of 204 final stalking-case decisions terminated proceedings for lack of offence elements [13]. Published data do not identify which element was missing; the figure cannot establish that harm was decisive. Judgments under Article 115 illustrate the difficulty of sanctioning pursuit without an explicit threat [26–29]. Alternative specified consequences or an endangerment model warrant consideration.

3. Article 127-2 protects minors against bullying, whereas Article 131 requires an indecent form of insult [3; 4]. Sustained harassment of adults that does not satisfy threat, stalking, insult or privacy-offence elements may therefore fall outside these provisions [15]. A separate administrative offence concerning adult harassment could close this gap; Table 1 distinguishes it from related offences.

4. Legal prohibitions require effective detection, content removal and preservation of proof. Algorithms may flag abusive material [20], and Kazakhstan uses an interagency removal mechanism [2]. Yet removal can erase evidence [19], and filtering must protect expression [12]. The examined cases rely on digital messages and recordings [26; 27]. Platforms and operators should be required to preserve removed content and metadata for a defined period, subject to procedural safeguards.

Discussion

Adapting inherited legal categories to an information society is not a one-off drafting exercise; it is an ongoing process, and Kazakhstan's terminology for online aggression is still, in a fairly literal sense, being assembled in real time. What follows sets domestic statutory language against the doctrinal vocabulary that has taken shape internationally, in order to see where the two overlap and where they diverge.

Doctrinal approaches to the concept of digital violence. International scholarship has largely settled on "technology-facilitated abuse" (TFA) as the umbrella category. A global Delphi study defines TFA as the misuse or repurposing of digital systems for the purposes of pursuit, coercion, or abuse. The category is deliberately broad – it is not confined to intimate-partner contexts but extends into workplaces, schools, and encounters between strangers. Four elements recur across the expert consensus reported in that study: the character of the perpetrator's conduct, the harm it inflicts, how the victim perceives that harm, and the absence of consent [17]. What distinguishes digital violence from its offline counterpart, on this account, is less its content than its reach: anonymity and constant accessibility mean the harm is no longer bound by physical distance from the aggressor.

Forms of digital violence identified in doctrine. Kazakhstani legal scholarship has produced its own typology. Nukusheva and co-authors distinguish several recurring patterns: flaming – rapid, emotionally charged public exchanges; harassment – persistent aggressive conduct directed at a specific individual; cyberstalking – pursuit of a victim through electronic communications; denigration – the circulation of misleading, degrading or accusatory material; outing – the unauthorized disclosure of personal information; and social exclusion or boycotting – the deliberate removal of a person from online groups and conversations. Even within Kazakhstani scholarship, the terminology has not stabilized: the same conduct – publishing defamatory material – is labelled "dissing" in one source [16] and "dissidence" in another [15], a small

inconsistency that nonetheless underscores how badly a legally binding definition is needed. Doctrine also places cyberflashing – sending intimate images without the recipient's consent – within this category [17; 18], alongside online grooming – building a relationship of trust with a child for purposes of later sexual exploitation [12; 21].

Statutory definitions in Kazakhstani law and their relationship to doctrine. Where doctrine builds a broad umbrella, the legislature has instead worked offence by offence. The concept of «bullying» first entered the statute book in 2022. Under sub-clause 4-1 of Article 1 of the Law «On the Rights of the Child in the Republic of Kazakhstan», bullying of a child is defined as «systematic (two or more) actions of a degrading character, pursuit and/or intimidation... including those committed through mass media and/or telecommunications networks and/or online platforms (cyberbullying)». That definition, in effect, narrows the doctrinal concept of cyberbullying down to the protection of minors alone. In criminal law, the online dimension of interpersonal violence is addressed through Article 115-1 of the Penal Code (stalking), defined as «the unlawful pursuit of a person, expressed in actions aimed at establishing contact and/or tracking a person against their will... resulting in substantial harm». Read against the doctrinal concept of "cyberstalking," this suggests that Kazakhstani law treats the digital method of commission as simply one possible mode of carrying out a broader general offence, rather than as a distinct category in its own right.

Interim conclusion. Taken together, these observations confirm that Kazakhstani law has no single generic term for digital violence. Criminalization proceeds piecemeal, and that piecemeal quality produces real difficulty when conduct directed at an adult falls short of stalking's threshold yet still amounts, in substance, to sustained online harassment. For the purposes of this study, digital violence is accordingly defined as the deliberate use of information and communication technologies to violate a person's psychological integrity, restrict their freedoms, or degrade their honour and dignity against their will [16; 17].

Criminal liability for stalking entered Kazakhstani law through the Law of the Republic of Kazakhstan of 16 July 2025 No. 210-VIII «On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Optimizing the Criminal Legislation of the Republic of Kazakhstan» [7]; Article 115-1 entered into force on 20 August 2025. The reform was meant to close a real protective gap around personal inviolability and to intervene before harassment escalates into serious violence, particularly within domestic settings, where persistent pursuit is often the precursor to more serious harm [9].

Object of the offence. The doctrine treats the generic object of the offence as the set of social relations that secure a person's rights and freedoms [14], while its direct object is more specifically personal liberty, privacy, and psychological integrity. Pursuit disturbs a person's peace of mind and encroaches on their constitutional right to communicate freely and to feel personally secure [9].

Objective element. Article 115-1 defines the conduct as follows: «Stalking, that is, the unlawful pursuit of a person, expressed in actions aimed at establishing contact and/or tracking a person against their will, not accompanied by violence, resulting in substantial harm». Four features together make up the objective side of the offence.

First, the mode of commission: the statute names two alternative forms of conduct – establishing contact (persistent calls, messages, letters) and/or tracking (surveillance, waiting outside a home or workplace). Second, unlawfulness and the absence of consent: the pursuit must occur «against the will» of the victim and lack any legal basis. Third, the absence of

physical violence: the norm is subsidiary and applies only where no signs of physical impact are present [9]; once violence enters the picture, the conduct is reclassified under other Penal Code provisions depending on its character and severity – for instance, under Article 107 (intentional infliction of moderate bodily harm) or Article 110 (torment). Fourth, the requirement of consequences: the offence is a material one and is considered complete only once substantial harm has actually occurred.

On the question of repetition, the text of Article 115-1 does not itself require systematicity. Doctrinal interpretation nonetheless treats pursuit as inherently repeated conduct by its nature: a single instance of unwanted attention does not amount to stalking [9].

Substantial harm as a consequence. The meaning of «substantial harm» is fixed by paragraph 14 of Article 3 of the Penal Code: consequences that, where not otherwise specified as an element of a particular offence, include violations of a person's or organization's constitutional rights and legitimate interests or of legally protected societal or state interests; the infliction of significant damage; the onset of a difficult life situation for the victim; disruption of an organization's or state body's normal functioning; or other consequences indicating that the harm caused is substantial. For stalking specifically, what matters most is establishing either a «difficult life situation» or a violation of the constitutional right to personal inviolability [9].

Subject and subjective element. The subject of the offence is a person of sound mind who has reached the age of sixteen (Article 15 PC RK). The subjective side requires intent: the offender must be aware that they are acting against the victim's will and must either desire the resulting harm or knowingly accept the risk of it.

Classification problems and the relationship to cyberstalking. Doctrine reads Article 115-1 as already encompassing cyberstalking – pursuit conducted through the internet, telecommunications networks, or other informatization objects, which may take the form of account hacking, the collection of personal data, the circulation of defamatory material, or manipulation carried out in digital environments [9; 15]. The practical difficulty lies in establishing a direct causal link between the perpetrator's digital conduct and the «substantial harm» required by the statute – proving, for example, that a stalker's online behaviour caused a diagnosable psychological disorder or forced the victim to change their way of life.

Law-enforcement practice under Article 115-1. The first months of application show both steady demand for the new norm and a high attrition rate at the pre-trial stage. According to the Investigation Department of the Ministry of Internal Affairs, by March 2026, 51 criminal cases of stalking had been sent to court, whereas in January 2026 only about eight cases had been initiated nationwide [24]. In Astana, 27 cases were registered by May 2026; courts delivered 13 convictions, and seven cases were terminated on non-exonerating grounds [25]. The most complete figures relate to the first five months of 2026: 248 criminal cases were registered under Article 115-1, final procedural decisions were taken in 204 of them, 83 cases were sent to court, 22 were terminated upon reconciliation of the parties, and 101 were terminated for lack of the elements of an offence [13].

These data should be read with caution. They are official figures released by state bodies through the media rather than the Committee's statistical reports; they do not separate online from offline pursuit; and they do not specify on which ground the absence of an offence was established – the lack of repetition, of the victim's objection, of intent or of substantial harm. Nevertheless, a termination rate of about one half of final decisions is high for an offence introduced precisely to allow early intervention, and it is consistent with the hypothesis that

the material construction of Article 115-1 filters out a considerable part of reported pursuit at the pre-trial stage. The Ministry of Internal Affairs itself has proposed reclassifying stalking as an offence of medium gravity with a qualifying feature of repetition, citing a case in the Almaty region where persons convicted of stalking continued the pursuit after conviction [13]. A reliable assessment will require a disaggregated analysis of termination decisions, which is identified below as a direction for further research.

Judicial practice under adjacent provisions: a case study. As of September 2026, judgments under Article 115-1 were not yet available in the open database of judicial acts. How pursuit-type conduct is treated in practice can nevertheless be seen from judgments under Article 115 of the Penal Code (threat), which before 20 August 2025 was the main instrument for responding to such conduct and which remains its closest neighbour. Four judgments delivered in 2025 are instructive.

In a case heard by the Zhetysu District Court No. 2 of Almaty, the defendant, a relative of the victim, sent him messages via WhatsApp over several weeks, also wrote to the victim's daughter, photographed the victim's car in the courtyard and threatened to burn it; a psychological and philological expert examination established the presence of threats and of degrading statements in the messages. The victim testified that his family had stopped moving freely in and out of the house and checked the entrance before leaving. The court convicted the defendant of threat, imposed 60 hours of community service and awarded 500,000 tenge in moral damages [26]. In a case heard by Aktobe City Court No. 2, the defendant, after a divorce, called the victim from hidden numbers, sent threatening messages through Instagram and – after she had blocked his numbers – through comments attached to small money transfers in a banking application, watched her house and approached her in a public place. He was found guilty of threat but released from criminal liability because the one-year limitation period for criminal misdemeanours had expired; the court imposed a one-year prohibition on contacting and pursuing the victim under Article 98-3 of the Penal Code [27].

In a case heard by the Ridder City Court, the defendant followed his former wife's car at night, blocked her way, threatened to kill her, and rammed her vehicle; the threat episode was punished by a fine, together with a one-year no-contact requirement [28]. Finally, in a case heard by the Talgar District Court, the defendant pursued a woman who had ended a relationship with him: he sent her threatening text messages, waited for her at her workplace first with a screwdriver and later with a knife; according to the victim's testimony, he also filed false reports to the police and repeatedly came to her parents' home, and she was forced to change her job. The court convicted him on two counts of threat and one count of arbitrariness and imposed 60 hours of community service [29].

The courts assessed discrete threats rather than pursuit as a course of conduct. In the Talgar case, pursuit occurred on 10–13 August 2025, before Article 115-1 entered into force, and preceded a forced change of employment [29]. Under Article 115, a perceived credible threat can be complete without ensuing harm [28]; prolonged pursuit under Article 115-1 requires substantial harm. The cases also illustrate the one-year limitation period for misdemeanours [27], reliance on digital messages and expert examination [26; 27], and the protective value of a prohibition on contacting or pursuing the victim under Article 98-3. They support reconsideration of the harm threshold and preservation of digital evidence.

Kazakhstani law currently splits the response to digital aggression between two branches – administrative and criminal – and that split makes precise delimitation between the two offences essential for correct classification of any given case.

Content and specifics of Article 127-2 of the Code of Administrative Offences. The special norm establishing liability for bullying entered the Code of Administrative Offences in 2024 [8]. Part 1 of Article 127-2 is framed simply as «Bullying (harassment, cyberbullying) of a minor». Its statutory content is fixed elsewhere, in sub-clause 4-1 of Article 1 of the Law «On the Rights of the Child in the Republic of Kazakhstan», which defines bullying of a child as «systematic (two or more) actions of a degrading character, pursuit and/or intimidation... committed publicly or through mass media and/or telecommunications networks and/or online platforms (cyberbullying)». The object protected by the norm is the rights, legitimate interests and safety of minors. The sanction under part 1 of Article 127-2 of the Code of Administrative Offences is «a warning or a fine of ten monthly calculation indices». A distinctive feature of the provision is that it reaches beyond the direct offender: where bullying is committed by a minor aged twelve to sixteen, the administrative penalty – warning or a fine of 10 MCI – falls on the parents or legal guardians instead [3; 15].

Content of Article 131 of the Penal Code (Insult). The Penal Code contains a general insult provision, defined as «the degradation of the honour and dignity of another person, expressed in an indecent form». Unlike the administrative offence, this norm protects any person regardless of age. Sanctions under Article 131 differ by part: part 1 carries «a fine of up to one hundred monthly calculation indices, or correctional labour in the same amount, or community service for up to one hundred and twenty hours», while part 2 – covering conduct committed publicly or through telecommunications networks or online platforms – carries «a fine of up to two hundred monthly calculation indices, or correctional labour in the same amount, or community service for up to one hundred and eighty hours».

The full text of Article 127-2 reads: «Article 127-2. Bullying (harassment, cyberbullying) of a minor. Bullying (harassment, cyberbullying) of a minor shall entail a warning or a fine of ten monthly calculation indices. The act provided for in part one of this Article, committed repeatedly within a year of an administrative penalty having been imposed, shall entail a fine of thirty monthly calculation indices. The act provided for in parts one or two of this Article, committed by a minor aged twelve to sixteen, shall entail a warning or a fine imposed on the parents or persons acting in their stead, in the amount of ten monthly calculation indices».

Criteria for distinguishing the two norms. Four criteria separate the offences. By the circle of protected victims, Article 127-2 protects only minors, whereas Article 131 protects any person. By the objective element, the administrative offence requires systematicity – two or more acts – while the criminal offence of insult can be committed in a single act [15]. By the form of expression, the criminal norm insists on an «indecent form» of degradation, while administrative bullying covers a wider range of conduct – pursuit, intimidation – that need not involve profanity at all [16]. And by the type of liability involved, the Code of Administrative Offences is oriented toward prevention and toward influencing legal guardians – including through the parental-liability mechanism for offenders aged twelve to sixteen – whereas the Penal Code pursues the ordinary aims of criminal punishment against accountable individuals aged sixteen and above.

The gap identified. What the *de lege lata* picture shows is that adults have no dedicated protection against comprehensive cyberbullying. Minors are covered by a purpose-built provision addressing bullying as an ongoing process, but adult victims are pushed toward Article 131, which is bound by the narrow «indecent form» requirement. Digital ostracism or coordinated psychological pressure directed at an adult therefore escapes legal evaluation entirely wherever it does not involve outright insult [16].

The proposed offence and its delimitation from related acts. In our view, the gap should be closed at the administrative rather than the criminal level. This preserves the coherence of the model created by Article 127-2, respects the principle of criminal law as a last resort, and creates a graduated scale of responses in which administrative liability addresses systematic harassment at an early stage, while the Penal Code comes into play where the conduct acquires the features of stalking, threat, insult or violation of privacy. We therefore propose supplementing the Code of Administrative Offences with a new article, «Harassment (cyberbullying) of a person who has reached the age of majority», with the following elements. The object is the honour, dignity, psychological integrity and privacy of an adult. The objective side consists of systematic (two or more within one year) actions committed through telecommunications networks or online platforms against the will of the victim and taking one of the following forms: degrading statements or images; intimidation; dissemination of information about the person's private life or of their personal data; or deliberate, coordinated exclusion from online communities accompanied by degrading statements. The offence is formal: neither an indecent form of expression nor the occurrence of consequences is required. The subject is a natural person who has reached the age of sixteen; the subjective side is direct intent. The disposition should contain a subsidiarity clause – «if these actions do not contain the elements of a criminal offence». The proposed sanction is a fine of twenty monthly calculation indices and, for a repeated offence within a year after an administrative penalty, a fine of fifty monthly calculation indices or administrative arrest for up to ten days.

The delimitation of the proposed offence from related acts is summarized in Table 1. The decisive criteria are the content of the conduct, the presence of a threshold of consequences and the level of liability. Where the conduct includes a threat of killing, grave bodily harm or destruction of property, Article 115 of the Penal Code applies; where it consists in establishing contact with or tracking the victim and causes substantial harm, Article 115-1 applies; a degrading statement in an indecent form is covered by Article 131; and the unlawful collection or dissemination of information about private life falls under Article 147. In the case of an ideal concurrence, the criminal offence absorbs the administrative one by virtue of the subsidiarity clause. The proposed administrative offence thus covers the residual zone of systematic online harassment that does not reach the threshold of any of these criminal offences – precisely the zone in which adults are currently left without protection.

Table 1 – Delimitation of the proposed offence from related offences

Provision	Conduct	Threshold/ consequences	Distinction from the proposed offence
Proposed article of the CAO: harassment (cyberbullying) of an adult	Systematic (2) degrading statements, intimidation, disclosure of private information, coordinated exclusion – through ICT	Formal offence; no indecent form or consequences required	–
Art. 127-2 CAO – bullying of a minor	Systematic degrading actions, pursuit, intimidation, online or offline	Formal; systematicity (2)	Victim is a minor; any mode of commission

Art. 115-1 PC – stalking	Establishing contact and/or tracking against the victim's will, without violence	Material: substantial harm	Aimed at contact or tracking rather than degradation; requires substantial harm; criminal liability
Art. 115 PC – threat	Threat of killing, grave bodily harm, destruction of property by arson or other dangerous means	Formal: sufficient grounds to fear execution of the threat	Content of the threat; a single act suffices
Art. 131 PC – insult	Degradation of honour and dignity	Formal; indecent form required; aggravated if online	Requires indecent form; a single act suffices
Art. 147 PC – violation of privacy	Unlawful collection or dissemination of information on private life; violation of personal data legislation	As specified in the respective parts of the article	Object is privacy and personal data as such; no requirement of systematic degradation

Note – compiled by the authors on the basis of [3; 4; 6].

Latency and evidentiary difficulties. The Committee on Legal Statistics and Special Records of the Prosecutor General's Office recorded 121 offences related to the bullying of minors between January and October 2024; parents of offenders were fined in only four of those cases, and 70 cases were resolved with a warning [5]. These figures show how the norm is applied – predominantly through the mildest sanction – but they do not by themselves allow conclusions about the scale of latency or about the effectiveness of the provision: registration depends on the willingness of children, parents and schools to report and on police practice, and no representative victimization survey on cyberbullying in Kazakhstan has yet been published. What can be said is that the number of registered cases is small relative to the number of schoolchildren, which, together with the evidentiary obstacles – closed messenger communities and the reluctance of schools to publicize conflicts – makes a high level of latency plausible, though not proven. Establishing its actual extent requires victimization surveys, which lie beyond the scope of this study.

Looking at how other jurisdictions have criminalized digital forms of violence helps identify legal constructions that Kazakhstan's criminal law could usefully borrow. European statutes and leading scholarly proposals point in a fairly consistent direction: toward more specialized norms and toward lowering the evidentiary bar in cyberharassment cases.

Germany: Section 238 of the Criminal Code (Stalking – *Nachstellung*). The German Criminal Code punishes the unauthorized pursuit of another person in a manner suitable to impair that person's way of life not insignificantly – for instance by seeking proximity, attempting contact through telecommunications, misusing personal data, or threatening the person or their relatives. Since the reform of 2017 the actual occurrence of a serious impairment is no longer required: it is sufficient that the conduct is objectively capable of producing it. The basic offence carries up to three years' imprisonment; especially serious cases, including those committed

by means of a computer program designed to spy on other persons' digital data, carry from three months to five years [22]. What stands out in the German approach is its emphasis on the systematic character of the conduct and on its potential effect on the victim's way of life – a standard considerably broader than the traditional focus on physical harm.

Italy: Article 612-bis of the Penal Code (*atti persecutori*). Italy's model of criminalizing stalking, introduced in 2009, is particularly instructive from a digitalization standpoint. Article 612-bis punishes repeated threats or harassment that produce one of three alternative consequences: a lasting and serious state of anxiety or fear; a well-founded fear for the safety of the victim or a close person; or a forced change in the victim's living habits. Like its Kazakhstani counterpart, the Italian offence is therefore result-based rather than formal; unlike it, however, it replaces an open evaluative notion of harm with a closed list of consequences that are typical of stalking and can be proved by the victim's testimony and circumstantial evidence. The penalty is increased where the act is committed through computer or telematic means [23] – a legislative judgment that digital forms of pursuit carry heightened social danger in their own right.

France: digital pursuit as an aggravating circumstance. French law was among the first to attach enhanced liability specifically to pursuit carried out through digital means. Law No. 2014-873 of 4 August 2014 introduced the offence of moral harassment in Article 222-33-2-2 of the Penal Code, under which committing the act against a minor, or through public online services, is treated as an aggravating circumstance. Researchers note that this approach formally recognizes children harassed online as victims and imposes stricter liability than for comparable offline conflicts [16]. Comparative EU studies also identify France as a jurisdiction with well-developed child-friendly civil remedies and a national anti-cyberbullying strategy [12].

The European Union: the BIK strategy and the Digital Services Act. At EU level, digital violence is approached primarily through the lens of children's rights and platform accountability. The "Better Internet for Kids" (BIK) strategy and the Digital Services Act (DSA) set normative expectations for child-friendly complaint mechanisms and transparent content-removal procedures. The DSA imposes horizontal obligations on platforms to provide easily accessible notice-and-action systems and transparent complaint-handling processes. This model shifts the centre of gravity away from criminal prosecution alone and toward building a safer digital environment through institutional filters and victim support [12].

A consent-based model for criminalizing cyberflashing. Professor Clare McGlynn argues for shifting away from a «motive-based» model of criminalizing digital violence toward one grounded in consent. Examining cyberflashing – the unsolicited sending of intimate images – she criticizes approaches that require proof of a specific motive on the perpetrator's part (an intent to cause distress or achieve sexual gratification, for instance), since this creates what she calls insurmountable evidentiary barriers. Her *de lege ferenda* proposal is to treat the act itself – the deliberate, non-consensual sending of such images – as a completed offence, since it violates "sexual autonomy and dignity" regardless of the sender's underlying motive [18].

Comparative conclusions and *de lege ferenda* proposals for Kazakhstan. The German and Italian models suggest specifying alternative consequences to "substantial harm" under Article 115-1, such as a forced change in the victim's way of life or persistent anxiety [9]. The gap in protection for adults supports an age-inclusive administrative bullying provision [16; 17]. A consent-based offence could address unsolicited intimate material [18]. Online commission could be considered as an aggravating feature of stalking, following the Italian model.

Feasibility of reception. Kazakhstan's separate category of criminal misdemeanours, one-year limitation period, general statutory definition of substantial harm and existing administrative protection of minors condition any borrowing from foreign law. Table 2 identifies each potentially transferable element and its necessary adaptation.

Table 2 – Foreign models and the feasibility of their reception into Kazakhstani law

Model	Key feature	What can be received	Adaptation to Kazakhstani law / limits
Germany, § 238 StGB [22]	Conduct "suitable" to impair the victim's way of life; actual harm not required; aggravation for use of spyware	"Suitability" construction as an alternative to substantial harm; aggravating feature of covert access to the victim's devices or data	Suitability defined through objective criteria (duration, frequency, intrusion into home or devices); basic form remains a criminal misdemeanour; German sanctions not borrowed
Italy, art. 612-bis c.p. [23]	Closed list of three alternative consequences; aggravation for computer or telematic means	Replacement of "substantial harm" in Art. 115-1 by a list of consequences; qualifying feature of commission through telecommunications networks or online platforms	Consequences proved by testimony and psychological examination, not by medical diagnosis; a moderate option that keeps the material construction
France, art. 222-33-2-2 C. pén. [10; 16]	Age-neutral moral harassment; aggravation for online commission and for concerted (group) harassment	Age-neutral concept of harassment; recognition of coordinated online harassment	Received at the administrative level (proposed CAO article), since gradation by health damage does not fit the category of criminal misdemeanours
England and Wales, s. 66A SOA 2003 [18; 32]	Specific offence of sending images of genitals; requires proof of purpose or recklessness	Specific offence of cyberflashing	Consent-based model without a motive element, avoiding the evidentiary problem criticized by McGlynn
EU: DSA; e-Evidence Regulation [11; 30]	Notice-and-action procedures; preservation orders with fixed periods	Fixed retention periods; formal preservation request; transparency of removal	Implemented through the Law on Online Platforms and the CPC; the supranational enforcement architecture is not transferable

Note – compiled by the authors.

Legal prohibitions alone cannot keep pace with the speed at which digital aggression unfolds; effective counteraction to cyberbullying increasingly depends on pairing normative rules with algorithmic monitoring systems and clear legal channels of interaction with online platforms.

Automated detection and severity-classification technologies. Doctrine has been actively exploring deep-learning approaches to identifying cyberbullying. One technical-legal study proposes a detection model built on a recurrent neural network with a Long Short-Term Memory (LSTM) architecture comprising four hidden layers; tested on a dataset of 47,733 Twitter comments, the model achieved a reported accuracy of 93.67%. To address the inherently subjective nature of what counts as bullying, the same study layers a fuzzy-logic algorithm on top of the LSTM output, using the count of offensive words to classify severity as low, medium or high, and benchmarks the results against alternative architectures such as DEA-RNN [20]. Tools of this kind could plausibly serve as a first line of early detection, catching aggression before it produces serious harm to minors.

Extrajudicial content-removal mechanisms: Kazakhstan and the EU compared. Identifying unlawful content is only half the task; there also has to be a procedural or administrative channel for removing it quickly. Kazakhstan has built a notice-and-takedown mechanism of its own. Under rules approved by the Ministry of Culture and Information, a dedicated interagency expert panel reviews complaints of cyberbullying against children. Complaints – which may be filed by the child, a legal guardian, or a third party – must be reviewed within three working days, extendable to fifteen in complex cases; once a case of cyberbullying is confirmed, the authorized body issues a binding order to the website or social-network owner requiring removal of the content [2].

This domestic mechanism sits conceptually close to the "notice-and-action" system established under the EU's Digital Services Act [11]. Under the DSA, digital platforms carry direct legal obligations to run transparent complaint-handling procedures, provide easily accessible mechanisms for reporting unlawful content, and guarantee effective access to remedies [12].

The problem of lost digital evidence. Automated detection and rapid takedown mechanisms create a serious procedural headache of their own for investigators: the irretrievable loss of digital traces. Platforms' internal moderation rules typically call for the swift removal of violent or graphic material, with the result that law-enforcement bodies may never even learn that an offence occurred. Worse, once content is taken down by a technology company, there is often no transparency about what happens to the underlying data or whether it is retained at all – meaning that crucial digital evidence can simply disappear. International criminal-law scholarship stresses the urgent need to develop legal cooperation mechanisms with social networks to guarantee evidence preservation and its transfer to investigative bodies and courts [19].

Balancing effectiveness against individual rights. What this analysis suggests is that criminal and administrative norms – including Article 127-2 of the Code of Administrative Offences and Article 115-1 of the Penal Code – need to function as part of an integrated technological infrastructure rather than in isolation from it. At the same time, automated detection and extrajudicial blocking carry their own risks. Algorithms are not immune to false positives, and opaque content removal by platforms not only destroys the evidentiary basis needed to hold offenders accountable but also risks unjustified restrictions on freedom of expression [12; 19].

For Kazakhstan, a balanced *de lege ferenda* model would combine detection algorithms of the LSTM type and the active work of interagency notice-and-takedown panels with a mandatory procedural requirement that internet providers "freeze" and securely retain deleted digital

traces of cyberbullying, so that criminal or administrative sanctions against the aggressor remain a realistic prospect rather than a formal possibility undermined by lost evidence.

Specification of the proposals on cyberflashing and on evidence preservation. Cyberflashing is not currently covered by a specific norm. Article 311 of the Penal Code on the illegal distribution of pornographic materials protects public morality rather than the sexual autonomy of the recipient, and its application depends on expert classification of the material as pornographic; Article 131 requires an indecent form of degradation, which an image may or may not satisfy. We propose supplementing Chapter 2 of the Penal Code (offences against sexual inviolability and sexual freedom) with a criminal misdemeanour worded as follows: "Intentional sending to another person, by means of telecommunications networks or online platforms, of an image or video recording depicting genitals or sexual acts without the prior consent of the recipient to receive such material." The offence is formal and consent-based: the purpose of the sender is irrelevant to qualification but may be taken into account in sentencing, which avoids the evidentiary problem identified by McGlynn in the English model [18; 32]. Where the recipient is a minor, the conduct should be assessed under the existing provisions protecting minors from sexual abuse, which carry more severe sanctions.

A digital-evidence preservation obligation should cover platforms and telecommunications operators [35]. It should arise when potentially unlawful content is removed or blocked, whether voluntarily, after a complaint or under an official order. Content and metadata (account identifiers, IP addresses and time stamps) should be securely retained with a recorded hash for 180 days, extendable once by 90 days upon a criminal-process request, then deleted if not requested. EU preservation orders provide for 60 days plus a possible 30-day extension [30], while the Budapest Convention provides expedited preservation for up to 90 days [31]. The proposed longer period accounts for delayed reporting; its necessity remains a matter for legislative assessment.

Preservation alone does not make data admissible evidence. Transfer should follow a request or seizure decision under the Criminal Procedure Code, with safeguards for private communications [33]. A statutory preservation request could follow registration of a report in the Unified Register of Pre-trial Investigations. Retention must have a statutory basis under personal-data law [34], with restricted, logged access and oversight.

Conclusion

This study has shown that Kazakhstan has assembled one of the more developed legal frameworks against digital violence within the Central Asian region. The legislature has taken substantial and timely steps: a statutory definition of cyberbullying is now in place, administrative liability for the bullying of minors has been introduced (Article 127-2 of the Code of Administrative Offences), stalking has been criminalized as a criminal misdemeanor (Article 115-1 of the Penal Code), and a sub-statutory notice-and-takedown mechanism has been put into operation. At the same time, the hypothesis underlying this research has been borne out in full: however progressive these reforms are, the resulting system of legal measures remains fragmentary and requires a conceptual shift toward a genuinely unified model of personal protection.

The findings identify five related issues. Kazakhstani law has no unified concept of digital violence. Article 115-1's substantial-harm requirement may hinder early intervention; available termination figures are consistent with concern but do not prove its cause [13]. Article 127-2

protects minors, while Article 131 does not cover every form of sustained adult harassment [3; 4]. German, Italian and French approaches offer elements for reform, subject to adaptation to Kazakhstan's criminal and administrative systems. Finally, rapid removal and algorithmic detection must be paired with safeguards for expression and the preservation of digital evidence. The proposed statutory changes below address these gaps.

To address the gaps identified, this study proposes the following *de lege ferenda* measures: replacing the "substantial harm" requirement in Article 115-1 with a closed list of alternative consequences – such as a "forced change in the victim's way of life" or "a state of persistent anxiety and fear for one's safety" – or reconstructing the offence on the model of conduct suitable to cause such consequences; adding commission "through telecommunications networks or online platforms" as a qualifying feature of the offence under Article 115-1; introducing into the Code of Administrative Offences a separate, formal offence of harassment (cyberbullying) of an adult with a subsidiarity clause delimiting it from Articles 115, 115-1, 131 and 147 of the Penal Code; criminalizing cyberflashing as a consent-based criminal misdemeanour in Chapter 2 of the Penal Code; and establishing an obligation for owners of online platforms and telecommunications operators to preserve removed content and metadata for 180 days, extendable by 90 days, together with a "preservation request" procedure in the Criminal Procedure Code and safeguards under personal data legislation.

Future research in this area will depend heavily on the accumulation of empirical data. The most pressing directions are a systematic study of investigative and judicial practice under Article 115-1 as judgments become publicly available, a disaggregated analysis of the grounds on which stalking cases are terminated, victimization surveys measuring the actual prevalence of cyberbullying among children and adults, and ongoing monitoring of how effectively Article 127-2 functions in ensuring that offences committed in the digital environment do not go unpunished.

Funding. This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26106325).

Conflict of interest

The authors state that there are no potential or apparent conflicts of interest under this article.

Author contributions:

A. Muratova – developed the research concept and methodology, analysed the legislation of the Republic of Kazakhstan, and conducted the final scholarly review of the article;

L. Lantero – analysed foreign legislation and international practice, contributed to the comparative legal analysis, and helped draft the article;

N. Apsimet – collected and organised the research materials, analysed judicial practice, developed recommendations, and contributed to writing the article.

References

1. Sayadi, S. and Rostami, M. (2026) «Cyber victimization and academic well-being: the mediating role of self-esteem and perceived social support in high school students», *Cogent Education*, 13(1), article 2665875. DOI: 10.1080/2331186X.2026.2665875.

2. Tegizbekova, Z. and Sarsenbayev, T. (2026) «Combating Cyberbullying Among Children: A Comparative Legal Analysis of Kyrgyzstan and Kazakhstan», <https://doi.org/10.3390/laws15020014> // <https://www.mdpi.com/2075-471X/15/2/14>
3. Republic of Kazakhstan (2014) Code of the Republic of Kazakhstan on Administrative Offences of 5 July 2014 No. 235-V (as amended as of 11 June 2026). Available at: <https://adilet.zan.kz/rus/docs/K1400000235> (Accessed: 11.06.2026).
4. Republic of Kazakhstan (2014) Criminal Code of the Republic of Kazakhstan of 3 July 2014 No. 226-V (as amended as of 11 June 2026). Available at: <https://adilet.zan.kz/rus/docs/K1400000226> (Accessed: 11.06.2026).
5. Abdrakhman, N. (2025) «Bullying Without Borders», Novoe Pokolenie, 25 April. Available at: <https://np.kz/news/obshchestvo/proisshestiya/travlya-bez-granits> (Accessed: 10.07.2026).
6. Republic of Kazakhstan (2002) Law of 8 August 2002 No. 345 «On the Rights of the Child in the Republic of Kazakhstan» (as amended as of 30 December 2025). Available at: https://adilet.zan.kz/rus/docs/Z020000345_ (Accessed: 15.06.2026).
7. Republic of Kazakhstan (2025) Law of 16 July 2025 No. 210-VIII «On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan Concerning the Optimisation of Criminal Legislation». Available at: <https://adilet.zan.kz/rus/docs/Z2500000210> (Accessed: 08.07.2026).
8. Republic of Kazakhstan (2024) Law of 15 April 2024 No. 72-VIII «On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan Concerning the Protection of Women's Rights and Children's Safety». Available at: <https://adilet.zan.kz/rus/docs/Z2400000072> (Accessed: 11.06.2026).
9. Rakhmetov, S.M. (2025) «Criminal Liability for Stalking», PRG (Paragraf). Available at: https://prg.kz/document/?doc_id=35517014 (Accessed: 10.03.2026).
10. France (n.d.) French Penal Code (Code pénal). Légifrance. Available at: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037289658/ (Accessed: 10.03.2026).
11. European Parliament and Council of the European Union (2022) Regulation (EU) 2022/2065 of 19 October 2022 (Digital Services Act), Official Journal of the European Union, L 277, pp. 1–102.
12. Kovács-Szépölggyi, E., Molnár, B. and Szakács, B. (2026) 'Remedy? Child Rights, Access to Justice and Preventive Responses to Cyberbullying in the European Union', Societies, pp. 1–19.
13. Saktaganova, L. (2026) «Stalking: Between Law and Reality». ZanMedia, 12 June. Available at: <https://zanmedia.kz/stalking-mezhdu-zakonom-i-realnostyu/162068/> (Accessed: 15.06.2026).
14. Borchashvili, I.Sh. (2024) 'Commentary on the Criminal Code of the Republic of Kazakhstan (Special Part)', zakon.uchet.kz. Available at: https://zakon.uchet.kz/rus/docs/T9700167_1_/t97167_1.htm (Accessed: 04.03.2026).
15. Orsayeva, R.A. (2024) 'Cyberbullying Among Adolescents: Concept, Types, Causes, Consequences and Liability', Vestnik nauki i tvorchestva, pp. 13–20.
16. Nukusheva, A.A., Kuandykov, B.Zh. and Zhaylau, Zh. (2024) 'A Comparative Legal Analysis of Legislation Countering Cyberbullying Among School-Age Children in Contemporary Jurisdictions', Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan, 2(77), pp. 247–260. DOI: 10.52026/2788-5291_2024_77_2_247.
17. Koukopoulos, N., Janickyj, M. and Tanczer, L.M. (2026) 'Defining and Conceptualizing Technology-Facilitated Abuse (Tech Abuse): Findings of a Global Delphi Study', Journal of Interpersonal Violence, 41(1–2), pp. 249–275. DOI: 10.1177/08862605241310465.
18. McGlynn, C. (2022) 'Cyberflashing: Consent, Reform and the Criminal Law', The Journal of Criminal Law, 86(5), pp. 336–352. DOI: 10.1177/00220183211073644.

19. Zarmsky, S. (2024) 'Is International Criminal Law Ready to Accommodate Online Harm? Challenges and Opportunities', *Journal of International Criminal Justice*, 22(1), pp. 169–184. DOI: 10.1093/jicj/mqae013.
20. Obaid, M.H., Elkaffas, S.M. and Guirguis, S.K. (2024) 'Deep Learning Algorithms for Cyber-Bullying Detection in Social Media Platforms', *IEEE Access*. DOI: 10.1109/ACCESS.2024.3406595.
21. Arabayev, Ch.I., Maatov, I.S. and Suerkulov, U. (2025) 'Organisation of Prosecutorial Supervision over Compliance with Laws on the Information Security of Minors', *International Journal of Humanities and Natural Sciences*, 2–3(101), pp. 175–180. DOI: 10.24412/2500-1000-2025-2-3-175-180.
22. Germany (n.d.) German Criminal Code (Strafgesetzbuch – StGB). Federal Ministry of Justice. Available at: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (Accessed: 20.03.2026).
23. Ministero della giustizia (n.d.) 'Harassment – Art. 612 c.p. Stalking'. Available at: https://www.giustizia.it/giustizia/en/mg_2_5_12_1.wp?contentId=GLM1144708 (Accessed: 16.03.2026).
24. Tumashevich, D. (2026) 'More Than 50 Stalking Cases Have Reached the Courts in Kazakhstan', *Kursiv Media*, 17 March. Available at: <https://kz.kursiv.media/2026-03-17/dnlt-bolee-50-del-o-stalkinge-doshli-do-suda-v-kazakhstane/> (Accessed: 28.05.2026).
25. 'Twenty-Seven Criminal Stalking Cases Opened in Astana' (2026), *Zakon.kz*, 20 May. Available at: <https://www.zakon.kz/obshestvo/6518550-27-ugolovnykh-del-za-stalking-zaveli-v-astane.html> (Accessed: 28.05.2026).
26. Zhetysu District Court No. 2 of Almaty (2025) Judgment of 29 May 2025 No. 7560-25-00-1/157. Judicial Office of the Supreme Court of the Republic of Kazakhstan. Available at: <https://office.sud.kz> (Accessed: 17.03.2026).
27. Court No. 2 of Aktobe, Aktobe Region (2025) Judgment of 12 May 2025 No. 1511-25-00-1/287. Judicial Office of the Supreme Court of the Republic of Kazakhstan. Available at: <https://office.sud.kz> (Accessed: 17.03.2026).
28. Ridder City Court, East Kazakhstan Region (2025) Judgment of 15 July 2025 in Case No. 6324-25-00-1/45. Judicial Office of the Supreme Court of the Republic of Kazakhstan. Available at: <https://office.sud.kz> (Accessed: 17.03.2026).
29. Talgar District Court, Almaty Region (2025) Judgment of 12 September 2025 No. 1962-25-00-1/145. Judicial Office of the Supreme Court of the Republic of Kazakhstan. Available at: <https://office.sud.kz> (Accessed: 17.03.2026).
30. European Parliament and Council of the European Union (2023) Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders, *Official Journal of the European Union*, L 191, pp. 118–180.
31. Council of Europe (2001) Convention on Cybercrime (ETS No. 185), Budapest, 23 November. Available at: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=185> (Accessed: 26.04.2026).
32. United Kingdom (2003) Sexual Offences Act 2003, section 66A (inserted by the Online Safety Act 2023, section 187). Available at: <https://www.legislation.gov.uk/ukpga/2003/42/section/66A> (Accessed: 28.04.2026).
33. Ordayeva A., Shekerbekova M. , & Abutaeva C. (2025). Fundamentals and mechanisms of national legislation on the prevention of stalking violation of personal space. *BULLETIN of L.N. Gumilyov Eurasian National University Law Series*, 150(1), 191–206. <https://doi.org/10.32523/2616-6844-2025-150-1-191-206>
34. Republic of Kazakhstan (2013) Law of 21 May 2013 No. 94-V «On Personal Data and Their Protection». Available at: <https://adilet.zan.kz/rus/docs/Z1300000094> (Accessed: 17.05.2026).

35. Republic of Kazakhstan (2023) Law of 10 July 2023 No. 18-VIII «On Online Platforms and Online Advertising». Available at: <https://adilet.zan.kz/rus/docs/Z2300000018> (Accessed: 17.05.2026).

Information about the authors:

Muratova A.Zh. – PhD, Head of the Department of Criminal Law Disciplines, Faculty of Law, L.N. Gumilyov Eurasian National University, 2 Satpaeva Str., 010008, Astana, Kazakhstan

Lantero L. – PhD, Associate Professor, European Public Law Organisation, European Law and Governance School, Piazza di Porta Portese 6, 00153, Rome, Italy

Apsimet N.M. – corresponding author, PhD, Lecturer, Department of Criminal Law, Criminal Procedure and Criminalistics, Faculty of Law, Al-Farabi Kazakh National University, 71 Al-Farabi Avenue, 050040, Almaty, Kazakhstan

Муратова А.Ж. – PhD, Заң факультеті, Қылмыстық-құқық кафедрасының меңгерушісі, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сатпаев көшесі 2, 010008, Астана, Қазақстан

Лантеро Л. – PhD, доцент, Еуропалық қоғамдық құқық ұйымы, Еуропалық құқық және басқару мектебінің доценті, Пьяцца ди Порта Портезе 6, 00153, Рим, Италия

Әпсімет Н.М. – хат-хабар авторы, PhD, заң факультеті, Қылмыстық құқық, қылмыстық іс жүргізу және криминалистика кафедрасы оқытушы, Әл-Фараби атындағы Қазақ ұлттық университеті, әл-Фараби даңғылы, 71, 050040, Алматы, Қазақстан

Муратова А.Ж. – доктор PhD, заведующий кафедрой уголовно-правовых дисциплин, Юридический факультет, Евразийский национальный университет имени Л.Н. Гумилева, ул. Сатпаева, 2, 010008, Астана, Казахстан

Лантеро Л. – доктор PhD, доцент, Организация европейского публичного права, Школа европейского права и управления, Пьяцца ди Порта Портезе, 6, 00153, Рим, Италия

Апсимет Н.М. – автор для корреспонденции, доктор PhD, преподаватель кафедры уголовного права, уголовного процесса и криминалистики, Юридический факультет, Казахский национальный университет имени аль-Фараби, проспект аль-Фараби, 71, 050040, Алматы, Казахстан



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY NC) license (<https://creativecommons.org/licenses/by-nc/4.0/>).