https://doi.org/10.31489/2026L2/47-57
UDC 340.341
Received:16.02.2026 | Accepted:29.03.2026 | Published online:30.06.2026

D. Utegen*

Maqsut Narikbayev University, Astana, Kazakhstan
(E-mail: d_utegen@kazguu.kz)
ORCID ID: 0000-0001-5296-7916

Legal Limits on the Use of Digital Evidence in Cybercrime Cases: Examining the right to privacy in the EU, and the Republic of Kazakhstan

Cybercrime investigations increasingly rely on intrusive digital techniques that can interfere with private life. This article identifies minimum procedural safeguards that reconcile effective cybercrime enforcement with respect for privacy. Using doctrinal and comparative legal analysis, it benchmarks Kazakhstan's regulation of intrusive investigative measures against standards developed by the European Court of Human Rights and relevant European Union requirements, with reference to practices in selected member states. The study examines four techniques: interception of communications, access to traffic and location data, remote access to digital devices, and the use of commercial spyware. The comparison shows that vague statutory bases and weak supervision can turn crime-control tools into surveillance. At a minimum, privacy-compatible enforcement requires prior independent authorization, clear limits on scope and duration, auditable rules for data handling (storage, access, sharing, deletion), effective oversight and accountability, post-measure notification when it no longer jeopardizes investigations, and accessible remedies. The article concludes with priority reforms for Kazakhstan to strengthen legal certainty and oversight while preserving investigative capacity.

Keywords: cybercrime, surveillance, privacy, intrusive measures, metadata, digital evidence, proportionality, ECtHR, procedural safeguards, commercial spyware.

Introduction

Digital technology has expanded cybercrime and, at the same time, the investigative toolkit used to respond to it. Interception, covert device access and large-scale data collection often operate in secrecy and can cut deeply into private life. When the legal basis is drafted broadly or procedural checks are thin, legitimate investigation can slide into disproportionate interference. This article therefore maps the minimum legal and procedural safeguards that should accompany such measures, using European human rights jurisprudence and Kazakhstan's evolving regulatory framework as the core points of reference. It explains how the ECtHR has interpreted and adjusted the principles of proportionality and legal certainty under Article 8 of the ECHR. Scholars like Robert Alexy [1] and Aharon Barak [2] have shaped the test around legality, legitimate aim, necessity, and balancing. In surveillance law, there is an ongoing debate about how proportionality works in practice. Some focus on security and point to the scale and speed of cyber threats, arguing that broader legislative powers are needed, as Orin Kerr's flexible approach to digital searches demonstrates [3]. Others, including David Cole [4] and Neil Richards [5], warn that secrecy and technology gaps can lead to abuse. They call for stronger judicial oversight, narrower legal authorization, and strict safeguards before and after surveillance.

These disagreements surface in debates over bulk interception and metadata retention. Some say that communications metadata differs from content data and does not require strong safeguards. Others argue that metadata can reveal private information about people. European case law and academic writing increasingly support this view. There is also debate about how much freedom authorities should have in national security and cybercrime cases. Some scholars argue that greater flexibility is needed in complex situations. Others warn that excessive discretion can weaken legal standards and oversight. The literature is also split between those who focus on legal rules and those who use social or empirical methods to study safeguards in practice.

The biggest disagreements are about remote device access and commercial spyware. Unlike traditional interception, spyware can secretly and continuously collect a wide range of data from digital devices. Scholars writing on the Pegasus case and "mercenary surveillance", including Rowan Philp [6], argue that spyware blurs the line between targeted interception and general searches. This challenges current proportionality standards. They see spyware not only as more intrusive but also as a new kind of state power. They argue that this requires new safeguards.

* Corresponding author's e-mail: *d_utegen@kazguu.kz*

On the other hand, some scholars who focus on security see spyware as a more advanced version of existing investigative tools. They believe that current judicial approval systems can handle these technologies with proper oversight. The main debate is whether spyware should be regulated as interception or as a general digital search, given its broad, secretive nature. This issue relates to key principles established under Article 8 of the ECHR. These include foreseeability, scope limitations, effective oversight, and protection against abuse. It also ties into broader debates in surveillance studies. For example, David Lyon [7] analyzes how constant monitoring and counter-terrorism tools become standard law enforcement practices.

Even though research on this topic has grown since the Pegasus Project, there is still no clear way to link the level of technological intrusion to the safeguards needed. Most studies focus on exposing abuse or making broad human rights arguments. Few connect the European Court of Human Rights' proportionality rules to specific digital investigative powers. This article seeks to fill that gap by creating a system that aligns investigative measures with the core procedural protections in European human rights law. It explains how to balance effective investigations with the protection of private life under the rule of law. As surveillance expands, policymakers face a new challenge. How long can human rights principles stay strong if advanced spyware keeps moving faster than legal safeguards?

The demand for effective investigative tools is easy to understand when set against current incident levels. The UK Cyber Security Breaches Survey 2025 reports that 43 % of organisations experienced cyber incidents or attacks in the past year [8]. In Germany, studies on economic crime estimate annual losses of EUR 289.2 billion, with cyberattacks accounting for a substantial share [9].

In Kazakhstan, official Ministry of Internal Affairs reporting on the results of 2025 confirms both the scale and complexity of cyber-enabled offending. According to the Ministry, 40 % of all registered offences are fraud, and 60 % of those fraud cases are committed through the internet [10]. Year-end official reporting also states that 84.5 million fraudulent calls were blocked in 2025, 13 call centers were dismantled, and 56 criminal cases were investigated in relation to so-called "droppers" [11]. These figures help explain why investigations increasingly turn to privacy-intrusive measures such as interception, access to traffic and location data, covert monitoring, searches of digital devices, and, in some cases, commercial spyware.

The article proceeds in three steps. First, it summarizes the ECtHR's approach under Article 8 and the safeguards the Court expects for covert surveillance. Second, it reviews key EU requirements governing access to and retention of communications data. Third, it assesses Kazakhstan's rules on digital evidence and online investigative measures, read together with national cybersecurity policy.

In Kazakhstan, the relevant rules are dispersed across several intersecting regimes: national security, information and communication technologies (ICT) and information security regulation, criminal law on informatization and communications offences, and new digital regulation. Key instruments include the Law on National Security [12], Government Resolution No. 832 on ICT and information security [13], Chapter 7 of the Criminal Code [14], the Digital Code [15] and the Concept of Cyber Shield of Kazakhstan [16]. Taken together, these sources reflect a growing policy emphasis on strengthening investigative capacity while acknowledging constitutional limits and privacy safeguards.

Against that backdrop, the article specifies what "minimum safeguards" should mean in practice when digital evidence is collected through interception, access to metadata, remote device measures, or commercial spyware. The analysis uses ECtHR standards and EU member-state practice as benchmarks and then tests the Kazakh framework against them. The goal is practical: recommendations that increase legal certainty and oversight without weakening lawful cybercrime enforcement.

Future research can sharpen these findings by testing how safeguards operate in practice (for example, how authorisation, logging and oversight work in real investigations), by tracking new surveillance techniques, and by expanding the comparison to additional jurisdictions. Such work would help specify how security objectives can be pursued without normalising routine, unchecked intrusion into private life.

Methods and materials

The paper combines doctrinal analysis of legislation and case law with a structured comparison of safeguards across jurisdictions. For the ECtHR strand, the analysis focuses on Article 8 standards for secret surveillance and interception, with reference to *Klass and Others v. Germany*, *Roman Zakharov v. Russia*, and *Big Brother Watch and Others v. the United Kingdom*.

For the comparative strand, the article contrasts the EU, ECtHR standards and Kazakhstan across four dimensions: the legal bases for intrusive measures; the authorisation and oversight architecture; data-handling rules (retention, access and deletion); and available remedies. Alongside primary sources, the re-

view draws on secondary legal literature, policy analysis and publicly available materials on the deployment and regulation of mercenary spyware.

To connect doctrine with practice, the study also uses incident statistics, sector reports and publicly reported cases. The ECtHR tests of legality, legitimate aim, necessity and proportionality serve as the organising framework for assessing interception, metadata access, remote device measures and commercial spyware, and for identifying the safeguards that should accompany these powers.

Finally, the comparative findings are checked against publicly available information on cyber incidents and surveillance tools. This step reduces the risk of purely abstract conclusions and supports recommendations focused on legal certainty, independent oversight and workable safeguards for cybercrime investigations.

Results

Digital evidence in cybercrime cases ranges from basic requests for subscriber or IP information to highly intrusive measures such as real-time interception, remote device access, and large-scale or cross-border data acquisition. The degree of intrusion depends not only on whether content is accessed, but also on the breadth of associated communications data. Even where content is never read, metadata (time, location, duration and counterparties) can reveal sensitive aspects of private life.

Commercial surveillance software refers to tools produced by private vendors that covertly collect, extract or intercept data from devices. Products such as Pegasus and Predator are marketed as counter-terrorism and anti-crime tools, yet reporting across jurisdictions shows their use against journalists, activists, public figures and private citizens [17]. Because such tools can activate microphones and cameras, access media files and extract stored data without the user's knowledge, the resulting interference is often comprehensive rather than limited. Amnesty International's Security Lab published a forensic methodology report explaining technical traces associated with Pegasus infections and attempted infections [18].

Kazakhstan also illustrates these broader risks. Amnesty International reported Pegasus infections on the mobile devices of several Kazakhstani civil society activists in 2021. These episodes underline a practical gap between formal legal limits and effective oversight: where notification, transparency and independent control are weak, the risk of excessive or misdirected surveillance increases, and trust in digital investigations erodes [18].

On this basis, the investigative measures in cybercrime cases can be grouped by their level of intrusion. Each group is equipped with basic procedural safeguards, in line with ECtHR standards and common European practices.

1. Highly intrusive actions require prior independent authorization. This includes interception of communications, remote device access, or use of commercial spyware. These measures must rely on clear legal grounds, have strict time limits, and be overseen by an independent authority.

2. Moderately intrusive measures, such as the collection of metadata and limited access to communications data, must be guided by a clearly defined purpose and scope. These actions require established protocols for data minimization, retention, and deletion, as well as comprehensive audit trails.

3. Low-intrusiveness actions include requesting basic subscriber or IP information and using aggregated datasets. Clear guidelines must control data storage and deletion. When possible, notification and mechanisms for seeking remedies should be provided.

This classification clarifies each category and links it to minimum safeguards. It promotes legality, necessity, and proportionality. It also encourages transparency and public trust in cybercrime investigations.

On this basis, the article proposes a typology of investigative measures by intrusiveness and links each type to a baseline set of safeguards derived from ECtHR standards and European practice. The typology helps identify areas where the legal framework leaves broader discretion to investigative authorities.

A major challenge in legal regulation is distinguishing between traditional interception of communications and direct access to digital devices. Traditional interception is relatively well-regulated in many jurisdictions, including Kazakhstan. However, current legal policies usually lack explicit provisions for remote device access or government hacking. Such practices may constitute a significantly more intrusive form of surveillance.

Where these minimum safeguards are defined in law and applied in practice, digital evidence can be gathered effectively without undermining the right to private life. The comparative analysis therefore treats safeguards not as obstacles to investigations but as conditions for lawful evidence-gathering and for maintaining public trust in cybercrime enforcement.

These concerns are reflected in the legal tests applied in Europe. Under Article 8 of the ECHR [19], any interference with private life must be "in accordance with the law", pursue a legitimate aim (including the prevention of crime), and be "necessary in a democratic society". The ECtHR has consistently stressed that secrecy increases rather than reduces the need for "adequate and effective safeguards against abuse" [20]. In cybercrime investigations, operational efficiency therefore cannot substitute for a clear legal basis and robust procedural guarantees. Kazakhstan's constitutional framework also recognizes data protection. Since 1995, Article 18 of the Constitution guarantees privacy and the confidentiality of correspondence and communications, providing a baseline for assessing digital investigative powers [21]. In addition, constitutional amendments are currently under public and expert discussion: the published draft of the new constitutional text explicitly guarantees protection of personal data against unlawful collection, processing, storage, and use, including in the digital sphere, thereby elevating personal data protection to the constitutional level [22].

Kazakhstan's approach to cybersecurity law has evolved from fragmented regulations to a cohesive legal framework. Foundational legislation formed the basis for later advancements. A key milestone was the 2015 Law "On Informatization", establishing regulations for information systems, electronic resources, government databases, and information security [23]. The 2017 "Cyber Shield of Kazakhstan" [16] was built on these efforts by developing national protection for information infrastructure, enhancing cyber-resilience, and formalizing incident response. Its explicit policy objectives enabled the development of new institutions and legal instruments. Further progress came with the 2026 Digital Code of Kazakhstan, consolidating digital technology, data, information systems, and security regulations [15]. These developments show Kazakhstan's shift from fragmented to comprehensive digital and cybersecurity management. For cybercrime investigations, the key question becomes how these instruments translate into concrete limits, oversight and data-handling rules that protect privacy while allowing lawful evidence collection.

Applying the typology of digital investigative measures by level of intrusiveness helps analyze how Kazakhstani law provides procedural safeguards and highlights areas where officials have broad discretion. For highly intrusive actions like interception, spyware use, or remote device access, prior independent approval, legal grounds, strict time limits, and oversight are essential. Moderately intrusive measures, such as metadata or limited communications data collection, need a clear purpose and scope, rules for data minimization and deletion, and thorough audit trails. Less intrusive actions, such as requesting subscriber information or aggregated data, should follow transparent rules for information storage and deletion and provide notification and remedies where possible. Clearly stated and enforced safeguards allow authorities to lawfully collect evidence without violating privacy, fostering confidence in cybercrime enforcement.

Discussion

Judicial practice of the ECtHR

Privacy and freedom of expression may be restricted, but only under the established three-part test: the interference must be prescribed by law, pursue a legitimate aim, and be necessary and proportionate in a democratic society. "Prescribed by law" requires accessible and foreseeable rules and safeguards that constrain discretion, which is particularly important for covert surveillance. Necessity and proportionality require that any measure be tightly limited in scope and duration, subject to effective independent oversight and remedies, and applied without discrimination [20].

In cybercrime cases, the ECtHR is the key European benchmark for assessing covert surveillance under Article 8. Its judgments translate legality, necessity and proportionality into operational requirements for interception and other forms of digital data collection. Interception of content is treated as especially sensitive because it exposes intimate communications and is typically conducted in secrecy.

The Court's interception jurisprudence therefore insists on safeguards that make the circumstances and procedures foreseeable. Put differently, the legal framework must do more than authorise interception: it must embed controls that prevent routine or open-ended monitoring.

Klass and Others v. Germany and *Roman Zakharov* v. Russia illustrate this point [24, 25]. Both cases emphasise that interference must be "in accordance with the law", pursue a legitimate aim, and be accompanied by practical safeguards that make necessity and proportionality real rather than rhetorical. The Court points, for example, to limits on affected persons and qualifying *offences, time limits, retention and destruction rules, supervision arrangements and avenues for* challenge.

Big Brother Watch and Others v. the United Kingdom extends the same logic to bulk regimes. The Grand Chamber accepted that bulk interception is not automatically incompatible with the Convention, but it

required "end-to-end" safeguards: authorisation, selection, examination, storage and oversight must each be constrained and reviewable [26].

Cyber incidents create pressure for speed and technical sophistication. ECtHR case law nevertheless treats safeguards as non-negotiable. Operational convenience does not justify bypassing legality, independent authorisation, effective oversight or remedies, even in serious security contexts.

Across this jurisprudence, a recurring set of minimum safeguards can be distilled: accessible and foreseeable laws; limits on affected persons and qualifying offences; prior independent authorisation; strict time limits and clear extension rules; clear rules for handling, retaining and deleting collected data; independent oversight; and effective remedies and, where compatible with the investigation, notification.

The Grand Chamber in Big Brother Watch reaffirmed that even with bulk interception, "end-to-end" safeguards are required. These measures protect private life rights from authorization through data retention to subsequent oversight [26].

ECtHR practice also suggests that safeguards do not only protect privacy: they support the reliability of digital evidence and the legitimacy of enforcement. Conversely, episodes involving commercial spyware show how secrecy, weak oversight and limited transparency increase the risk of arbitrary interference and downstream evidentiary disputes.

Judicial practice of the European Union member states

Within the EU, rules on digital evidence operate alongside a broader data-protection and cybersecurity framework. The GDPR sets baseline requirements for lawful processing, storage and deletion of personal data and protects rights such as access, rectification and erasure [27]. In parallel, cybersecurity instruments (including NIS2) push organisations toward risk management, incident reporting and resilience measures [28].

European courts generally treat proportionality and independent control as the organising principles for digital evidence. They draw a clear line between indiscriminate surveillance and targeted monitoring: large-scale collection requires explicit legal authority, specified purposes and strong external oversight. Targeted measures, by contrast, are more easily justified when they rest on concrete suspicion and are time-bound.

Recent CJEU debates have been shaped by investigations into encrypted communication services, notably EncroChat and Sky ECC. These platforms offered modified devices and secure messaging that complicated conventional interception. Public reporting indicates that EncroChat had roughly 66,000 users across 122 countries before its 2020 dismantling and that investigators relied heavily on large datasets captured through technical operations.

The CJEU has not directly ruled on the substantive legality of the underlying hacks; its analysis has instead focused on the procedural conditions for cross-border use of the resulting data. On 30 April 2024, in Case C-670/22, M.N. (EncroChat), the Court considered whether European Investigation Orders (EIOs) issued by a German public prosecutor could be used to obtain EncroChat data collected in France.

The Court held that a public prosecutor may issue an EIO to request transfer of data already collected in another EU country, provided that the same rules would apply domestically and that national courts can review the measure for compliance with fundamental rights. It also clarified that Article 31 of Directive 2014/41/EU treats "interception of telecommunications" in functional terms, capturing operations that provide access to communications data regardless of the precise technical pathway.

As to remedies, the Court indicated that exclusion of evidence is not automatic even where violations are found. Admissibility remains largely governed by national law, but fair-trial rights set limits: if the defence cannot effectively test key evidence obtained through an EIO, a court may need to disregard that evidence to preserve fairness [29].

In Ekimdzhiev and Others v. Bulgaria, the Court determined that Bulgaria's surveillance and data retention framework lacked sufficient safeguards. Although nominally "targeted", ambiguous legal standards, restricted judicial oversight, and inadequate remedies rendered the regime comparable to mass surveillance. The Court underscored that the mere existence of such legislation may infringe upon privacy. Safeguards must be effective in practice rather than solely in theory [30].

In Tele2 Sverige and Watson, the CJEU held that European Union law prohibits indiscriminate data retention. Only targeted retention for the investigation of serious crime is permissible, provided it is subject to stringent conditions and prior review by a court or an independent authority. The Court established that mass data collection contravenes EU privacy standards, except in exceptional national security circumstances. Investigative access must be subject to robust independent oversight [31].

After Ekimdzhiev and Tele2, the Court further tightened access to communications metadata. In *H.K. v Prokuratuur*, it required prior independent authorization—preferably judicial—before law enforcement may access such data, save for genuine emergencies. Allowing prosecutors to authorise access on their own was found incompatible with proportionality and effective legal protection. Therefore, only an independent party may authorize access to communications metadata; this authority should not be granted to the public prosecutor [32].

In M.N. (EncroChat), the CJEU addressed cross-border use of previously collected EncroChat data. It confirmed that an EIO may be used to request transfer of such data and that prosecutors may issue EIOs where national law permits. Necessity and proportionality remain required; the Court indicated that individualized suspicion for every user is not always mandatory. It also recognised that confidentiality of hacking methods does not automatically bar evidence, provided defence rights are respected; where the defence cannot effectively challenge the material, exclusion may be necessary. The judgment reiterated notification duties in cases of transnational interception [33].

Taken together, these cases point to a pragmatic but rights-constrained line: large investigations and cross-border cooperation are possible, but only under a framework that preserves independent oversight and fair-trial guarantees. Admissibility is therefore linked to both the lawfulness of collection and the defence's ability to challenge it.

In this sense, proportionality and independent control are not abstract ideals but practical conditions for the sustainable use of digital evidence. Successes against encrypted-crime networks do not remove the need for targeted powers, clear legal authority, strict retention rules and effective remedies.

Digital Surveillance and Human Rights in Kazakhstan

Cybercrime and internet-enabled fraud remain a significant enforcement challenge in Kazakhstan, increasing the practical demand for reliable digital evidence collection and preservation. Official Ministry of Internal Affairs reporting indicates that fraud now accounts for 40 % of all registered offences in the country, and that 60 % of those fraud cases are committed through the internet. Year-end official reporting for 2025 also states that 84.5 million fraudulent calls were blocked, 13 call centers were dismantled, including centers operating abroad, and 56 criminal cases were under investigation in relation to so-called "droppers" [10, 11]. These indicators help explain why law-enforcement authorities increasingly rely on privacy-intrusive investigative tools such as interception, access to traffic and location data, covert monitoring, searches of digital devices, and other digital tracing measures. At the same time, broader official reporting on countering cybercrime shows the growing institutional emphasis on preventive, technical, and investigative responses, which further reinforces the need for clear legal bases, independent authorization, and effective oversight consistent with human rights standards [34].

Kazakhstan's rules on digital evidence are spread across national security legislation, information-security regulation and criminal procedure, which makes the framework difficult to navigate and weakens transparency for data subjects [35]. This fragmentation also complicates accountability: different bodies may rely on interception, remote device access or large-scale data collection without a single, legible set of procedural guarantees.

International and domestic law permit interference with private life only for limited aims (for example, national security or crime prevention) and only through procedures that make those limits operational. In Kazakhstan, the reported gap between formal rules and day-to-day practice points to deficits in transparency, notification and external control especially where intrusive measures are conducted covertly.

Kazakhstan's experience also mirrors a broader pattern: commercial spyware enables sophisticated surveillance with limited accountability. Tools originally developed for counter-terrorism have been documented as being used against journalists, activists and public figures in multiple countries [36]. Where procurement and deployment are opaque, it becomes difficult to assess legality, necessity and proportionality in concrete cases.

International responses to spyware are evolving. Courts and regulators in other jurisdictions have begun to impose consequences on vendors whose tools facilitate unlawful surveillance. For example, in 2025 a U.S. court ordered NSO Group to stop targeting WhatsApp users and addressed damages in related litigation [37]. Although the proceedings occurred outside Kazakhstan, they signal a wider regulatory shift toward vendor accountability.

Kazakhstan's information infrastructure also remains vulnerable to cyberattacks, as the 2024 iSoon data leak illustrated. Such incidents highlight how dependence on particular technology ecosystems can create

systemic exposure. From a safeguards perspective, they also matter because insecure systems amplify the harm of surveillance: data extracted unlawfully or retained excessively becomes easier to misuse or leak.

Against this background, Kazakhstan can strengthen the legal framework for digital surveillance through a small set of priority measures: require prior judicial authorization for the most intrusive powers; assign clear competence rules and independent oversight; set explicit limits on scope, duration and permissible methods; and adopt enforceable rules on storage, access, logging, deletion and, where compatible with investigations, notification. These measures are aimed at improving legality and accountability, not at constraining lawful cybercrime enforcement.

Beyond legal design, alignment with international standards depends on routine "effectiveness-and-rights" reviews of investigative powers, clear operational guidance and institutional capacity for oversight. The objective is straightforward: evidence should be obtained in a manner that courts can trust and that individuals can contest when limits are exceeded.

Conclusions

This article examined the expanding digital investigative powers in the context of cybercrime and assessed the safeguards required for privacy and human rights. A comparative analysis shows that digital evidence may be lawfully obtained only when intrusive powers are matched by enforceable safeguards. Both ECtHR and EU frameworks require prior independent authorization for intrusive measures, clear limits, effective oversight, strong data-handling requirements, and meaningful remedies. Without such safeguards, privacy is threatened and the legitimacy of enforcement undermined.

Kazakhstan has initiated reforms to align more closely with these standards, including adopting the Digital Code and enhancing constitutional protections for personal data. Article 18 of the Constitution safeguards the privacy of correspondence and personal data, while the Digital Code (2026) clarifies the management of data, digital technologies, information systems, and cybersecurity. Chapter 7 of the Criminal Code and Government Resolution No. 832 further delineate procedures for accessing digital data. Nevertheless, regulatory fragmentation and limited oversight continue to create legal uncertainty. To address this, Kazakhstan should prioritize establishing specific, enforceable rules for independent authorization, oversight, data retention and deletion, and accessible remedies based on ECtHR and EU benchmarks, ensuring clear and actionable protections for digital investigations.

A key contribution of this analysis is the typology that categorizes investigative powers by their level of intrusiveness and aligns each category with specific, actionable safeguards derived from ECtHR and EU practice. This framework offers policymakers a practical method for calibrating protections to the risks associated with different investigative measures.

As surveillance technologies evolve rapidly and operate across borders, legal frameworks require periodic review and recalibration. For Kazakhstan, the primary recommendation is to develop and rigorously implement a comprehensive system of independent authorization, clear procedures, and strong oversight mechanisms for digital investigations. This is essential for translating international best practices into effective, practical safeguards that maintain the balance between security and rights protection.

Ultimately, robust safeguards are not obstacles but the foundation of lawful and effective evidence-gathering, enabling sustainable cybercrime enforcement and fostering enduring public trust. As digital challenges accelerate, Kazakhstan's commitment to strong legal and institutional protections will determine its success in protecting both security and fundamental rights.

References

1 Alexy R. Constitutional rights, balancing, and rationality [Electronic resource] / R. Alexy // Ratio Juris. — 2003. — Vol. 16, No. 2. — P. 131–140. — Access mode: https://www.corteidh.or.cr/tablas/a63.pdf

2 Barak A. Proportionality and principled balancing [Electronic resource] / A. Barak // Law and Ethics of Human Rights. — 2010. — Vol. 4, No. 1. — P. 1–16. — Access mode: https://philpapers.org/rec/BARPAP-5

3 Kerr O.S. Searches and seizures in a digital world [Electronic resource] / O.S. Kerr // Harvard Law Review. — 2005. — Vol. 119, No. 2. — P. 531–585. — Access mode: https://www.jstor.org/stable/4093493

4 Cole D. Preserving privacy in a digital age: Lessons of comparative constitutionalism [Electronic resource] / D. Cole // Georgetown Law Faculty Publications and Other Works. — 2013. — Access mode: https://scholarship.law.georgetown.edu/facpub/1310/

5 Richards N.M. (2013). The dangers of surveillance / N.M. Richards // Harvard Law Review. — Vol. 126, No. 7. — P. 1934–1965.

6 Philp R. “Chasing shadows”: How a small civil society investigative team is fighting the growing cyber surveillance threat [Electronic resource] / R. Philp // Global Investigative Journalism Network. — 2025. — Access mode: https://gijn.org/stories/ron-deibert-chasing-shadows-book-cyber-surveillance-threats/

7 Lyon D. Surveillance after September 11 [Electronic resource] / D. Lyon // Sociological Research Online. — Vol. 6, No. 3. — 2001. — Access mode: https://journals.sagepub.com/doi/abs/10.5153/sro.643

8 Cyber Security Breaches Survey 2025. — 2025. — [Electronic resource]. — Access mode: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

9 Cyber attacks cost the German economy 300 billion euros in the past year, survey finds. Reuters. — 2025. — [Electronic resource]. — Access mode: https://www.reuters.com/world/china/cyber-attacks-cost-german-economy-300-bln-euros-past-year-survey-finds-2025-09-18/

10 Министерство внутренних дел Республики Казахстан. 95 % уголовных дел в стране расследуются органами внутренних дел. — 2026. — [Электронный ресурс]. — Режим доступа: https://www.gov.kz/memleket/entities/qriim/press/news/details/1132076? lang=ru

11 Министерство внутренних дел Республики Казахстан. От профилактики к цифровой трансформации: МВД подвело итоги 2025 года и определило приоритеты на предстоящий период. — 2026. — [Электронный ресурс]. — Режим доступа: https://www.gov.kz/memleket/entities/qriim/press/news/details/1139163? lang=ru

12 Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан». — 2012. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/Z1200000527

13 Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». — 2016. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P1600000832

14 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V. — 2014. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/K1400000226

15 Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII. — 2026. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/K2600000255

16 Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)». — 2017. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P1700000407

17 Amnesty International. Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally. — 2021. — [Electronic resource]. — Access mode: https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

18 Amnesty International. Kazakhstan: Four activists’ mobile devices infected with Pegasus spyware. — 2021. — [Electronic resource]. — Access mode: https://www.amnesty.org/en/latest/news/2021/12/kazakhstan-four-activists-mobile-devices-infected-with-pegasus-spyware/

19 European Convention on Human Rights. Council of Europe. — 1950. — [Electronic resource]. — Access mode: https://www.echr.coe.int/documents/d/echr/convention_ENG

20 Balancing data protection with transparent justice: The European legal framework. The AIRE Centre. — 2023. — [Electronic resource]. — Access mode: https://www.rolplatform.org/wp-content/uploads/2023/11/balancing-data-protection-with-transparent-justice-eng.pdf

21 Конституция Республики Казахстан. — 1995. — [Электронный ресурс]. — Режим доступа: https://www.akorda.kz/en/constitution-of-the-republic-of-kazakhstan-50912

22 Проект новой Конституции Республики Казахстан. — 2022. — [Электронный ресурс]. — Режим доступа: https://www.gov.kz/memleket/entities/mfa-minsk/documents/details/967814? lang=ru

23 Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации». — 2015. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000418

24 Klass and Others v. Germany (Application no. 5029/71): Judgment of the European Court of Human Rights. — 1978. — [Electronic resource]. — Access mode: https://hudoc.echr.coe.int/eng? i=001-57510

25 Roman Zakharov v. Russia (Application no. 47143/06): Judgment of the European Court of Human Rights, December 4, 2015. — [Electronic resource]. — Access mode: https://hudoc.echr.coe.int/eng? i=001-159324

26 Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14, 24960/15): Judgment of the European Court of Human Rights, May 25, 2021. — [Electronic resource]. — Access mode: https://hudoc.echr.coe.int/eng? i=001-210077

27 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). — 2016. — [Electronic resource]. — Access mode: https://eur-lex.europa.eu/eli/reg/2016/679/oj

28 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). — 2022. — [Electronic resource]. — Access mode: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

29 Cybercrime Judicial Monitor, Issue 10. (2025, July). — [Electronic resource]. — Access mode: https://www.eurojust.europa.eu/sites/default/files/assets/files/cybercrime-judicial-monitor. -issue-10.pdf

30 Ekimdzhiev and Others v. Bulgaria (Application no. 70078/12): Judgment of the European Court of Human Rights. — 2022. — [Electronic resource]. — Access mode: https://hudoc.echr.coe.int/eng? i=001-214673

31 Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others: Judgment of the Court of Justice of the European Union. — 2016. — [Electronic resource]. — Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX:62015CJ0203

32 Case C-746/18, H.K. v Prokuratuur: Judgment of the Court of Justice of the European Union. — 2021. — [Electronic resource]. — Access mode: https://curia.europa.eu/juris/document/document.jsf? docid=240390&doclang=EN

33 Case C-670/22, Criminal proceedings against M.N. (EncroChat): Judgment of the Court of Justice of the European Union. — 2024. — [Electronic resource]. — Access mode: https://curia.europa.eu/juris/document/document.jsf? docid=285368&doclang=EN

34 Министерство внутренних дел Республики Казахстан. Противодействие киберпреступности. — 2025 — [Электронный ресурс]. — Режим доступа: https://www.gov.kz/memleket/entities/qriim/activities/25086? lang=ru

35 Utegen D. Kazakhstan needs tougher laws to address the impacts of spyware [Electronic resource] / D. Utegen. — 2022. — Access mode: https://optf.ngo/blog/kazakhstan-needs-tougher-laws-to-address-the-impacts-of-spyware

36 Reuters. U.S. court orders spyware company NSO to stop targeting WhatsApp; reduces damages — 2025. — [Electronic resource]. — Access mode: https://www.reuters.com/sustainability/society-equity/us-court-orders-spyware-company-nso-stop-targeting-whatsapp-reduces-damages-2025-10-18/

37 Китайская хакерская группировка контролировала критические объекты IT-инфраструктуры Казахстана. — 2024. — [Электронный ресурс]. — Режим доступа: https://cert.kz/news/chinese-hacker-group-controlled-critical-it-infrastructure-facilities-in-kazakhstan/

Д. Өтеген

Киберқылмыс істеріндегі цифрлық дәлелдемелерді пайдаланудың құқықтық шектері: Еуропалық одақ және Қазақстан Республикасы тәжірибесінде жеке өмірге қол сұқпаушылық құқығын талдау

Киберқылмыстарды тергеу барған сайын жеке өмірді құрметтеу құқығына елеулі қол сұғатын цифрлық тәсілдерге сүйенеді. Мақала киберқылмыстарды тиімді қадағалауда жеке салаға қол сұғылмаушылықты сақтай отырып, үйлестіруге мүмкіндік беретін ең төменгі іс жүргізу кепілдіктерін анықтайды. Доктриналық және салыстырмалы-құқықтық талдау арқылы Қазақстан Республикасындағы инвазивті тергеу шараларының құқықтық режимі Адам құқықтары жөніндегі Еуропалық соттың практикасы, Еуропалық одақтың талаптары және Еуропалық одаққа мүше жекелеген мемлекеттердің тәжірибесімен жүйелі түрде салыстырылады. Төрт кең таралған әдіс қарастырылды: хабарламаларды қолға түсіру, трафик пен орналасу деректеріне қол жеткізу, сандық құрылғыларға қашықтан қол жеткізу және коммерциялық шпиондық бағдарламалық жасақтаманы қолдану. Талдау құқықтық негіздің бұлыңғырлығы мен бақылаудың жеткіліксіздігі қылмысқа қарсы шараларды бақылау құралдарына айналдыруға қабілетті екендігін көрсетеді. Құқық қолданудың жеке өмірге қол сұғылмаушылық құқығымен үйлесімділігі, кем дегенде, алдын ала тәуелсіз рұқсат алумен, тақырыпқа нақты шектеулер мен мерзімдермен, деректермен жұмыс істеудің тексерілетін ережелерімен (сақтау, қол жеткізу, беру, жою), тиімді қадағалау және есеп беру, бұл тергеуге қауіп төндірмейтін шара аяқталғаннан кейін тұлғаға хабарлау және қолжетімді құқықтық қорғау құралдары арқылы қамтамасыз етіледі. Қорытындыда Қазақстан үшін құқықтық айқындық пен қадағалауды күшейтетін, бірақ тергеу әлеуетін сақтайтын басым реформалар ұсынылады.

Кілт сөздер: киберқылмыс, бақылау, жеке өмір, интрузивті шаралар, метадеректер, цифрлық дәлелдемелер, пропорционалдық, ЕАҚС, процессуалдық кепілдіктер, коммерциялық шпиондық бағдарламалар.

Д. Утеген

Правовые пределы использования цифровых доказательств по делам о киберпреступлениях: обеспечение права на неприкосновенность частной жизни в практике ЕС и Республики Казахстан

Расследования киберпреступлений всё чаще опираются на инвазивные цифровые методы, способные существенно затрагивать право на уважение частной жизни. Статья определяет минимальные процессуальные гарантии, позволяющие сочетать эффективное преследование киберпреступлений с соблю-

дением неприкосновенности приватной сферы. На основе доктринального и сравнительно-правового анализа проводится сопоставление правового режима Республики Казахстан с подходами Европейского суда по правам человека и требованиями Европейского союза с учётом практик отдельных государств — членов Европейского союза. Рассматриваются четыре распространённые техники: перехват сообщений, доступ к данным трафика и местоположения, удалённый доступ к цифровым устройствам и применение коммерческого шпионского программного обеспечения. Показано, что расплывчатые правовые основания и недостаточный контроль способны превращать меры борьбы с преступностью в инструменты наблюдения. Совместимость правоприменения с правом на частную жизнь обеспечивается, как минимум, предварительным независимым санкционированием, чёткими пределами по предмету и срокам, проверяемыми правилами обращения с данными (хранение, доступ, передача, уничтожение), эффективным надзором и отчётностью, уведомлением лица после завершения меры, когда это не ставит под угрозу расследование, и доступными средствами правовой защиты. В заключение предлагаются приоритетные реформы для усиления правовой определённости и контроля при сохранении следственного потенциала.

Ключевые слова: киберпреступность; наблюдение; частная жизнь; интрузивные меры; метаданные; цифровые доказательства; пропорциональность; ЕСПЧ; процессуальные гарантии; коммерческое шпионское ПО.

References

1 Alexy, R. (2003). Constitutional rights, balancing, and rationality. *Ratio Juris, 16*(2), 131–140. Retrieved from https://www.corteidh.or.cr/tablas/a63.pdf

2 Barak, A. (2010). Proportionality and principled balancing. *Law and Ethics of Human Rights, 4*(1), 1–16. Retrieved from https://philpapers.org/rec/BARPAP-5

3 Kerr, O.S. (2005). Searches and seizures in a digital world. *Harvard Law Review, 119*(2), 531–585. Retrieved from https://www.jstor.org/stable/4093493

4 Cole, D. (2013). Preserving privacy in a digital age: Lessons of comparative constitutionalism. *Georgetown Law Faculty Publications and Other Works*. Retrieved from https://scholarship.law.georgetown.edu/facpub/1310/

5 Richards, N.M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934–1965.

6 Philp, R. (2025). "Chasing shadows": How a small civil society investigative team is fighting the growing cyber surveillance threat. *Global Investigative Journalism Network*. Retrieved from https://gijn.org/stories/ron-deibert-chasing-shadows-book-cyber-surveillance-threats/

7 Lyon, D. (2001). Surveillance after September 11. *Sociological Research Online, 6*(3). Retrieved from https://journals.sagepub.com/doi/abs/10.5153/sro.643

8 (2025). Cyber Security Breaches Survey 2025. *gov.uk*. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

9 (2025). Cyber attacks cost the German economy 300 billion euros in the past year, survey finds. Reuters. *reuters.com*. Retrieved from https://www.reuters.com/world/china/cyber-attacks-cost-german-economy-300-bln-euros-past-year-survey-finds-2025-09-18/

10 (2026). Ministerstvo vnutrennikh del Respubliki Kazakhstan. 95 % ugolovnykh del v strane rassleduiutsia organami vnutrennikh del [95 % of criminal cases in the country are investigated by internal affairs bodies]. *gov.kz*. Retrieved from https://www.gov.kz/memleket/entities/qriim/press/news/details/1132076? lang=ru [in Russian].

11 (2026). Ministerstvo vnutrennikh del Respubliki Kazakhstan. Ot profilaktiki k tsifrovoi transformatsii: MVD podvelo itogi 2025 goda i opredelilo prioritety na predstoiashchii period [From prevention to digital transformation: The MIA summarized its 2025 results and identified priorities for the coming period]. *gov.kz*. Retrieved from https://www.gov.kz/memleket/entities/qriim/press/news/details/1139163? lang=ru [in Russian].

12 (2012). Zakon Respubliki Kazakhstan ot 6 yanvaria 2012 goda No. 527-IV «O natsionalnoi bezopasnosti Respubliki Kazakhstan» [Law of the Republic of Kazakhstan No. 527-IV of January 6, 2012 "On National Security of the Republic of Kazakhstan"]. *adilet.kz*. Retrieved from https://adilet.zan.kz/rus/docs/Z1200000527 [in Russian].

13 (2016). Postanovlenie Pravitelstva Respubliki Kazakhstan ot 20 dekabria 2016 goda No. 832 «Ob utverzhdenii edinykh trebovanii v oblasti informatsionno-kommunikatsionnykh tekhnologii i obespecheniia informatsionnoi bezopasnosti» [Resolution of the Government of the Republic of Kazakhstan No. 832 of December 20, 2016 on approval of unified requirements in the field of information and communication technologies and information security]. *adilet.kz*. Retrieved from https://adilet.zan.kz/rus/docs/P1600000832 [in Russian].

14 (2014). Ugolovnyi kodeks Respubliki Kazakhstan ot 3 iiulia 2014 goda No. 226-V [Criminal Code of the Republic of Kazakhstan No. 226-V of July 3, 2014]. *adilet.kz*. Retrieved from https://adilet.zan.kz/rus/docs/K1400000226 [in Russian].

15 (2026). Tsifrovoi kodeks Respubliki Kazakhstan ot 9 yanvaria 2026 goda No. 255-VIII [Digital Code of the Republic of Kazakhstan No. 255-VIII of January 9, 2026]. *adilet.kz*. Retrieved from https://adilet.zan.kz/rus/docs/K2600000255 [in Russian].

16 (2017). Postanovlenie Pravitelstva Respubliki Kazakhstan ot 30 iiunia 2017 goda No. 407 «Ob utverzhdenii Kontseptsii kiberbezopasnosti («Kibershchit Kazakhstana»)» [Resolution of the Government of the Republic of Kazakhstan No. 407 of June 30,

2017 on approval of the Cybersecurity Concept ("Cyber Shield of Kazakhstan")]. *adilet.kz*. Retrieved from https://adilet.zan.kz/rus/docs/P1700000407 [in Russian].

17 (2021). Amnesty International. Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally. *amnesty.org*. Retrieved from https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

18 (2021). Amnesty International. Kazakhstan: Four activists' mobile devices infected with Pegasus spyware. *amnesty.org*. Retrieved from https://www.amnesty.org/en/latest/news/2021/12/kazakhstan-four-activists-mobile-devices-infected-with-pegasus-spyware/

19 (1950). European Convention on Human Rights. Council of Europe. *echr.coe.int*. Retrieved from https://www.echr.coe.int/documents/d/echr/convention_ENG

20 (2023). Balancing data protection with transparent justice: The European legal framework. The AIRE Centre. *rolplatform.org*. Retrieved from https://www.rolplatform.org/wp-content/uploads/2023/11/balancing-data-protection-with-transparent-justice-eng.pdf

21 (1995). Konstitutsiia Respubliki Kazakhstan [Constitution of the Republic of Kazakhstan]. *akorda.kz*. Retrieved from https://www.akorda.kz/en/constitution-of-the-republic-of-kazakhstan-50912 [in Russian].

22 (2022). Proekt novoi Konstitutsii Respubliki Kazakhstan [Draft of the New Constitution of the Republic of Kazakhstan]. *gov.kz*. Retrieved from https://www.gov.kz/memleket/entities/mfa-minsk/documents/details/967814? lang=ru [in Russian].

23 (2015). Zakon Respubliki Kazakhstan ot 24 noiabria 2015 goda No. 418-V «Ob informatizatsii» [Law of the Republic of Kazakhstan No. 418-V of November 24, 2015 on Informatization]. *adilet.kz*. Retrieved from https://adilet.zan.kz/rus/docs/Z1500000418 [in Russian].

24 (1978). Klass and Others v. Germany (Application no. 5029/71): Judgment of the European Court of Human Rights. *hudoc.echr.coe.int*. Retrieved from https://hudoc.echr.coe.int/eng? i=001-57510

25 (2015). Roman Zakharov v. Russia (Application no. 47143/06): Judgment of the European Court of Human Rights. *hudoc.echr.coe.int*. Retrieved from https://hudoc.echr.coe.int/eng? i=001-159324

26 (2021). Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14, 24960/15): Judgment of the European Court of Human Rights. *hudoc.echr.coe.int*. Retrieved from https://hudoc.echr.coe.int/eng? i=001-210077

27 (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *eur-lex*. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

28 (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *eur-lex*. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2555/oj

29 (2025). Cybercrime Judicial Monitor, Issue 10. Eurojust. *eurojust.europa.eu*. Retrieved from https://www.eurojust.europa.eu/sites/default/files/assets/files/cybercrime-judicial-monitor. -issue-10.pdf

30 (2022). Ekimdzhiev and Others v. Bulgaria (Application no. 70078/12): Judgment of the European Court of Human Rights. *hudoc.echr.coe.int*. Retrieved from https://hudoc.echr.coe.int/eng? i=001-214673

31 (2016). Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others: Judgment of the Court of Justice of the European Union. *eur-lex*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX:62015CJ0203

32 (2021). Case C-746/18, H.K. v Prokuratuur: Judgment of the Court of Justice of the European Union. *curia.europa.eu*. Retrieved from https://curia.europa.eu/juris/document/document.jsf? docid=240390&doclang=EN

33 Case C-670/22, Criminal proceedings against M.N. (EncroChat): Judgment of the Court of Justice of the European Union, April 30, 2024. *curia.europa.eu*. Retrieved from https://curia.europa.eu/juris/document/document.jsf? docid=285368&doclang=EN

34 (2025). Ministerstvo vnutrennikh del Respubliki Kazakhstan. Protivodeistvie kiberprestupnosti [Countering cybercrime]. *gov.kz*. Retrieved from https://www.gov.kz/memleket/entities/qriim/activities/25086? lang=ru [in Russian].

35 Utegen, D. (2022). Kazakhstan needs tougher laws to address the impacts of spyware. *optf.ngo*. Retrieved from https://optf.ngo/blog/kazakhstan-needs-tougher-laws-to-address-the-impacts-of-spyware

36 (2025). Reuters. U.S. court orders spyware company NSO to stop targeting WhatsApp; reduces damages. *reuters.com*. Retrieved from https://www.reuters.com/sustainability/society-equity/us-court-orders-spyware-company-nso-stop-targeting-whatsapp-reduces-damages-2025-10-18/

37 (2024). Kitaiskaia khakerskaia gruppirovka kontrolirovala kriticheskie obekty IT-infrastruktury Kazakhstana [Chinese hacker group controlled critical IT infrastructure facilities in Kazakhstan]. *cert.kz*. Retrieved from https://cert.kz/news/chinese-hacker-group-controlled-critical-it-infrastructure-facilities-in-kazakhstan/ [in Russian].

Information about the author

Utegen Dana — PhD candidate, Maqsut Narikbayev University, Astana, Kazakhstan; e-mail: d_utegen@kazguu.kz