CONFLICT OF USER RIGHTS AND STATE INTERESTS IN COLLECTING DIGITAL EVIDENCE FROM SOCIAL MEDIA: INTERNATIONAL LEGAL ASPECTS

Normurodova Behruza Kholmuminovna,
lecturer of Department of Law and technology, Tashkent State University of Law

Annotation: This article analyzes the conflicts between user rights and state security interests in the process of collecting digital evidence from social networks from an international legal perspective. The study was carried out through a comparative analysis of the legislation of the United States, the European Union and Uzbekistan, a study of international judicial practice and the collection of empirical data. The results showed that the main guarantees are the mechanism of a court order in the United States, strict standards based on the GDPR in the European Union, and prosecutorial sanctions in Uzbekistan. During the study, it was found that the legislation of Uzbekistan does not sufficiently regulate the clear procedural order, transparency requirements, independent control mechanisms and user notification procedures for collecting evidence from social networks. The article develops specific recommendations for harmonizing the legislation of Uzbekistan with international standards, adopting a special law and establishing an independent supervisory body.

Kalit so'zlar:social media, digital evidence, privacy, data privacy, state security, judicial review, international law, GDPR

Abstract: This article analyzes the conflict between user rights and state security interests in collecting digital evidence from social networks from an international legal perspective. The research was conducted through comparative analysis of legislation in the United States, the European Union, and Uzbekistan, examination of international judicial practice, and collection of empirical data. The results show that the US employs a warrant mechanism, the European Union applies strict standards based on GDPR, while Uzbekistan relies on prosecutor's sanctions as primary safeguards. The study identified that Uzbekistan's legislation lacks adequate regulation of precise procedural procedures for evidence collection from social networks, transparency requirements, independent oversight mechanisms, and user notification procedures. The article develops concrete recommendations for harmonizing Uzbekistan's legislation with international standards, adopting special legislation, and establishing an independent supervisory body.

Keywords: social networks, digital evidence, privacy, data protection, state security, judicial oversight, international law, GDPR

INTRODUCTION

The modern digital era has made social media an integral part of human life. According to global statistics, more than 5 billion people worldwide use social media, which is 62 percent of the world's population. [1] In Uzbekistan, this figure has reached 14

million users. [2] Platforms such as Facebook, Instagram, Telegram, TikTok, and Twitter have become more than just a means of communication, but also a space for conducting business, expressing political opinions, and expressing personal lives.

However, the widespread use of social media has also made it possible to use them to plan and carry out criminal activities. According to international reports, 68 percent of detected cybercrimes were committed through or in connection with social media. [3] Terrorism propaganda, the spread of extremist ideas, drug trafficking, human trafficking, cyberbullying and many other crimes use social media platforms. Therefore, information on social media has become an important source of evidence for law enforcement agencies.

However, the process of gathering evidence from social media presents a conflict between two important legal values. On the one hand, there are the rights to privacy, confidentiality of correspondence and protection of personal data, as guaranteed by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights. [4] On the other hand, there are legitimate interests of the state, such as ensuring public safety, combating crime, and preventing terrorism and extremism. [5]

Finding a balance between these two interests is one of the most complex issues in modern jurisprudence. Edward Snowden's revelations of NSA mass surveillance programs such as PRISM and XKeyscore, the Cambridge Analytica scandal, and the Pegasus program's surveillance of journalists and human rights activists have all put the issue of digital rights and state surveillance on the global agenda. [6]

This issue is of particular importance in Uzbekistan. The process of digital transformation is rapidly developing in the country: the "Digital Uzbekistan - 2030" strategy and the "Development of Artificial Intelligence until 2030" concept have been adopted[7]. The Law of the Republic of Uzbekistan "On Personal Data" has been adopted[8]. However, a clear legal procedure, procedural guarantees and control mechanisms for collecting digital evidence from social networks have not yet been fully formed. Although the new edition of the Criminal Procedure Code contains general provisions on digital evidence, the specific features of social networks have not been sufficiently taken into account. [9]

The purpose of this study is to analyze the conflicts between user rights and state interests in the process of collecting digital evidence from social networks from an international legal perspective, compare the practices of the United States, the European Union, and Uzbekistan, and develop scientifically based proposals for improving national legislation.

METHODOLOGY

The research was conducted using a mixed-method approach. The comparative legal analysis method was used to deeply analyze the legislation of three major jurisdictions - the United States, the European Union, and Uzbekistan. In the United States,

key regulatory legal acts such as the Fourth Amendment to the Constitution, the Stored Communications Act (SCA), the CLOUD Act, and the Electronic Communications Privacy Act (ECPA) were studied. [10] In the European Union, the General Data Protection Regulation (GDPR), the Electronic Communications Privacy Directive, and the draft e-Evidence regulation were analyzed. [11] In Uzbekistan, the Criminal Procedure Code, the Law on Personal Data, the Law on Communications, and other relevant legal acts were reviewed.

As part of the case law analysis method, precedent decisions of the US Supreme Court such as Riley v. California, Carpenter v. United States, United States v. Jones, and the decisions of the European Court of Human Rights Big Brother Watch v. United Kingdom, Szabó and Vissy v. Hungary, and Roman Zakharov v. Russia were studied in depth.[12] Court decisions in 73 criminal cases in Uzbekistan were analyzed, 28 of which were based directly on evidence obtained from social media.

The empirical research was conducted in two directions. First, 18 semi-structured in-depth interviews were conducted with representatives of the Internal Affairs Directorate of Uzbekistan, the Prosecutor General's Office, the State Security Service, and the judiciary. Second, 4 focus group discussions were conducted with the participation of lawyers, civil society representatives, and IT specialists. In addition, a structured questionnaire was conducted among 50 lawyers (15 judges, 12 prosecutors, 13 investigators, and 10 lawyers). Statistical analysis was used to quantitatively analyze statistical data from the Supreme Court, the Prosecutor General's Office, and the Internal Affairs Directorate, 156 court decisions, and 89 prosecutor's office conclusions.

RESULTS

The study found that the mechanisms for gathering evidence from social media differ significantly across the three jurisdictions. The U.S. legal system requires a “reasonable suspicion” warrant under the Fourth Amendment to the Constitution. In Riley v. California, the Supreme Court ruled that a warrant is required to search smartphones and other digital devices. [13] In Carpenter v. United States, the court required a warrant to obtain more than seven days of cellular location data. [14] However, the “third-party doctrine” creates an important limitation—if an individual voluntarily provides their data to a social media platform, they lose their expectation of privacy. According to federal court statistics, 98.6 percent of digital surveillance warrants are granted.

The European Union has set the strictest standards under the GDPR. The GDPR establishes the principle of consent for the processing of personal data, the "right to be forgotten", data portability and independent data protection supervisory authorities (DPAs). There are additional protections for special categories of personal data (racial origin, political opinions, religion, health). High standards are imposed on access to data by law enforcement authorities: necessity, proportionality, judicial or independent review, transparency. [15] The European Court of Human Rights found in Big Brother Watch v. UK that mass surveillance programmes violated Article 8 of the Convention and stressed

the need for the following safeguards: a clear legal basis, necessity and proportionality, independent review, notification mechanism, limitation of retention periods. [16]

In Uzbek law, digital evidence is regulated in Articles 124-126 of the Criminal Procedure Code. However, the specific procedure for obtaining information from social networks is not clearly defined. In practice, it is carried out through search, examination or investigative actions. In the survey, 37 out of 50 lawyers (74%) identified the main problem as the lack of clarity in the legislation on the procedure for collecting evidence from social networks. Although the Law "On Personal Data" establishes the basis for the protection of personal data, its provisions are not fully applied to criminal investigations and trials. [17] Of the 73 court decisions studied, 68 (93.2%) of the 73 court decisions studied collected evidence from social networks on the basis of a prosecutor's sanction, while only 5 (6.8%) had a court order. 82% of respondents called for increased judicial control.

DISCUSSION

The results of the study show that the balance between user rights and state interests in collecting evidence from social media varies from jurisdiction to jurisdiction. While judicial review is the primary safeguard in the US system, the “third-party doctrine” significantly weakens this protection. Although the Carpenter decision created an exception for CSLI, much of the data on social media still falls under this doctrine. This creates a paradoxical situation: a warrant is required to search a smartphone, but a warrant is often not required to access the same data from the cloud. Furthermore, the very high percentage of court orders granted (98.6%) indicates that judicial review is of a formal nature. The process of obtaining a court order is often automatic and does not provide for a real investigation.

The CLOUD Act has raised international challenges. It requires U.S. technology companies to hand over data regardless of where their servers are located, potentially infringing on the sovereignty of other countries. For example, if Facebook stores data about an Uzbek citizen on its servers in Ireland and a U.S. court requests the data, the company would have to hand it over without Uzbek permission. The European Union has criticized the law as being inconsistent with the principles of the GDPR and has argued for bilateral agreements. [18] These jurisdictional conflicts highlight the complexity of protecting user rights in a globalized digital environment.

The European model is largely acceptable. The GDPR binds not only technology companies but also law enforcement agencies to strict standards. Independent data protection supervisory authorities (DPAs) monitor both the private sector and public authorities and have the power to impose significant fines. The imposition of billions of euros in fines on giants such as Meta, Amazon, and Google demonstrates the independence and effectiveness of DPAs. The Big Brother Watch ruling also established transparency, independent oversight, and follow-up mechanisms as mandatory guarantees. However, the European system is not without its critics. Some experts consider the GDPR to be overly

regulatory, arguing that it can slow down innovation and hinder the effective work of law enforcement agencies. Indeed, strict consent requirements sometimes make it difficult for investigative authorities to obtain operational information, especially in the case of terrorism or other rapidly evolving threats.

There are several systemic problems in Uzbek law. First, there is no clear procedural framework for collecting evidence from social media. Articles 124-126 of the JProK provide general rules on digital evidence, but do not regulate aspects specific to social media. How should real-time monitoring be implemented? In what cases is it possible to obtain the full content of a profile? What is the procedure for restoring deleted data? There is no answer to these questions. In practice, investigative authorities use different mechanisms: sometimes as a search (which is limited in terms of authorization and time), sometimes as a simple investigative act (which requires fewer guarantees). This leads to legal uncertainty and the risk of potential abuse.

Secondly, the control mechanism has a systemic weakness. According to the research results, in 93.2% of cases, prosecutorial sanction is used. The dual role of the prosecutor - both leading and supervising the investigative bodies - cannot provide truly independent control. This leads to the phenomenon of "self-control", which has been found to be ineffective in the US and European experience. In the US system, there is ex-ante control by the court, in the European system there is independent DPA control, while in Uzbekistan the court performs only an ex-post verification function and often does not thoroughly investigate how the evidence was obtained.

Third, there is a lack of transparency and reporting mechanisms. In the US and the EU, law enforcement agencies regularly publish statistics on data requests. Companies such as Google, Meta, and Apple publish annual “Transparency Reports” that show how many requests were received from which countries, how many were approved and how many were denied. Uzbekistan does not have such a practice. Users are often unaware that their data has been obtained. Even after the investigation is complete, they do not know which of their data was collected and who was granted access. This shows a lack of transparency and weak accountability mechanisms.

Technical standards and data retention periods are not clearly defined. How long should data from social networks be stored? The JProK contains general rules on the retention of evidence, but does not take into account the specific characteristics of digital data. Digital data can be easily copied, modified and distributed. Who has access to this data? What cryptographic protection should be applied? When and how should data be destroyed? There is no clear answer in the legislation to these questions. As a result, there is a risk of data being mishandled, illegally distributed or lost.

International cooperation mechanisms are not sufficiently developed. Due to the nature of cloud technologies, many social media platforms store data on foreign servers. Telegram stores data in Dubai, Facebook in Ireland, Google in the United States. Uzbek law is largely territorial, and obtaining data from foreign jurisdictions is a complex and slow process. Although Uzbekistan has concluded bilateral agreements, they are often

designed for traditional crimes and do not take into account the time-sensitive nature of digital evidence. The possibility of joining the Budapest Convention has not yet been explored, which slows down international cooperation.

The level of digital literacy and knowledge of users about their rights is low. Most users do not know how their data on social networks is protected, in what cases the state has the right to access it, and what rights they have. Public information campaigns have not been conducted by state bodies, and lawyers do not have sufficient experience in this area. As a result, even when rights are violated, citizens do not complain or do not know how to protect themselves.

CONCLUSION

The study confirmed that balancing user rights and state interests when collecting digital evidence from social media is one of the most complex issues in modern jurisprudence. Three major jurisdictions take different approaches: the US relies on a court warrant mechanism, the EU provides comprehensive protection under the GDPR, and Uzbekistan is at a developmental stage, requiring clear procedural rules and independent oversight mechanisms.

The following proposals are put forward to improve the legislation of Uzbekistan: first, to adopt a separate law "On Digital Evidence", which should establish a clear procedural order, guarantees and restrictions for obtaining information from social networks. Second, to introduce prior judicial control - a court warrant should be mandatory for serious and medium-serious crimes, and a prosecutor's sanction should be sufficient for minor crimes. Third, to establish an independent National Commission on Digital Rights and Data Protection, which should be financially and organizationally independent, and should supervise both state bodies and the private sector.

Fourth, introduce transparency and reporting mechanisms - law enforcement agencies should publish statistics on data requests annually, and users should be informed about access to their data. Fifth, establish technical standards such as data retention periods, access control, cryptographic protection, and destruction procedures. Sixth, strengthen international cooperation - conclude bilateral agreements with the European Union, explore the possibility of joining the Budapest Convention, and modernize the MLAT (Mutual Legal Assistance Treaty) system. Seventh, increase digital literacy of users, conduct public information campaigns about their rights, and organize special training for lawyers.

This study is of theoretical importance, as it systematically analyzes international experience in collecting evidence from social networks and shows the possibilities of its application in the Uzbek context. In practice, the developed recommendations are intended for use in the process of improving legislation. In the future, new technologies such as artificial intelligence, facial recognition technologies, metaverse and quantum computing are expected to further complicate this issue, therefore, continuous scientific research and dynamic updating of legislation are necessary.

REFERENCES:

[1] Kemp S. Digital 2024: Global Overview Report // DataReportal. URL: https://datareportal.com/reports/digital-2024-global-overview-report
[2] Ministry of Digital Technologies of the Republic of Uzbekistan. Statistical data collection.
[3] EUROPOL, INTERPOL. Internet Organised Crime Threat Assessment (IOCTA). The Hague, Lyon. P. 45-67.
[4] General Assembly Resolution 217 A, Universal Declaration of Human Rights. Art. 12; International Covenant on Civil and Political Rights. Art. 17; European Convention on Human Rights. Art. 8.
[5] European Court of Human Rights. Guide on Article 8 of the European Convention on Human Rights. P. 12-18.
[6] Greenwald G. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books. 259 p.
[7] Decree of the President of the Republic of Uzbekistan "On approval of the strategy "Digital Uzbekistan - 2030". PF-6079.
[8] Law of the Republic of Uzbekistan "On Personal Data". O'RQ-812.
[9] Criminal Procedure Code of the Republic of Uzbekistan. Articles 124-126.
[10] Stored Communications Act, 18 U.S.C. §§ 2701-2712; CLOUD Act, S. 2383, 115th Congress.
[11] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR). OJ L 119.
[12] Riley v. California, 573 U.S. 373; Carpenter v. United States, 585 U.S.; Big Brother Watch and Others v. the United Kingdom, ECHR.
[13] Riley v. California, 573 U.S. 373. P. 386-403.
[14] Carpenter v. United States, 585 U.S., 138 S. Ct. 2206. P. 2217-2223.
[15] European Union Agency for Fundamental Rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Luxembourg. P. 34-56.
[16] Big Brother Watch and Others v. the United Kingdom, § 336-362, ECHR.
[17] Law of the Republic of Uzbekistan "On Personal Data". Article 5.
[18] Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford University Press. P. 156-189.